# STUDIES ON PERFORMANCE OF WIRELESS SENSOR NETWORK USING TRUST BASED ROUTING PROTOCOLS

**THESIS**

*Submitted by*

**P.SAMUNDISWARY**

*in partial fulfilment for the award of the degree*

*of*

**DOCTOR OF PHILOSOPHY**

**in**

**ELECTRONICS AND COMMUNICATION ENGINEERING**


**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**
**PONDICHERRY ENGINEERING COLLEGE**
**PONDICHERRY UNIVERSITY**
**PONDICHERRY-605 014**
**INDIA**

**DECEMBER 2010**

**Dr.P.DANANJAYAN**
Professor
Department of Electronics and Communication Engineering
Pondicherry Engineering College
Pondicherry- 605 014.

## CERTIFICATE

Certified that this thesis entitled "**STUDIES ON PERFORMANCE OF WIRELESS SENSOR NETWORK USING TRUST BASED ROUTING PROTOCOLS"** submitted for the award of the degree of **DOCTOR OF PHILOSOPHY** in ELECTRONICS AND COMMUNICATION ENGINEERING of the Pondicherry University, Pondicherry is a record of original research work done by **Mrs. P.SAMUNDISWARY** during the period of study under my supervision and that the thesis has not previously formed the basis for the award to the candidate of any Degree, Diploma, Associateship, Fellowship or other similar titles. This thesis represents independent work on the part of the candidate.

**Supervisor**

**(Dr.P.Dananjayan)**

**Date:**

**Place: Pondicherry**

# ABSTRACT

The underlying vision for the emerging wireless communication system is to enable communication with a person, at any time, at any place and in any form. During the past decade, a surge of research activities have been witnessed in the field of wireless communication due to a confluence of several factors. First, there has been an explosive increase in demand for tether less connectivity, driven so far mainly by cellular telephony but now eclipsed by wireless multimedia applications. Secondly, the dramatic progress in semiconductor technologies, digital switching techniques and digital signal processing algorithms has facilitated the employment of wireless communication in large scale. These trends are anticipated to continue at a greater pace during the next decade.

The interest of scientific and industrial community in the realm of wireless communication not only alleviates the problem of wired traditional networks but also, has introduced two different types of communication such as cellular and adhoc networking. In cellular network, mobile units communicate with the base station via wireless link by exploiting the frequency reuse concept to serve unlimited number of users. This cellular network is often called as infrastructured network that connects the base station either to another base station or to public telephone network via switching center. On the other hand, the adhoc network architecture is an infrastructure less network which is used to set up a network rapidly when needed. The adhoc network is a collection of two or more mobile devices equipped with wireless communication and networking capability. In the adhoc networking paradigm, the packets are delivered to the destinations through wireless multihop connectivity and without any fixed infrastructure. The flexible and adaptive networking architecture of adhoc networks fulfill the requirements of various applications such as tactical communications and military networks.

A Wireless Sensor Network (WSN) is also considered as an adhoc network in which nodes are extended with sensing capability. The sensor network is composed of one or multiple sinks and many tiny, low power sensor nodes. These sensor nodes are devices used to monitor and gather the environmental information

which is then reported to remote sinks. The functionalities of a remote sink are to collect data from sensor nodes and to transmit commands to the sensor nodes. The nodes of WSN are randomly deployed in harsh environment for detecting and tracking the passage of troops and tanks on a battlefield and measuring the traffic flows on roads. So, the sensing nodes are prone to different types of routing attacks. The various routing attacks are spoofed routing information attack, HELLO flood attack, sybil attack, selective forwarding attack, sinkhole/black hole attack and worm hole attack. These attacks disrupt the routing mechanism of WSN by compromising the benevolent nodes. These compromised nodes mortify the performance of routing protocols of WSN. Therefore, different security mechanisms are needed for self organizing mobile WSN to prevent these attacks.

The security schemes which are used for conventional computer networks are not applicable to WSN because of its low powered batteries, lack of memory and increased scalability. Secured routing protocols using cryptographic techniques, hash functions and key predistributions schemes have been suggested to eliminate the routing attacks of WSN. These secured routing protocols require higher energy consumption, greater design complexity, increased memory capacity and high communication overhead, which are impractical in resource constrained WSN. Hence, it is intended to develop trust based routing protocols for WSN having mobile nodes to achieve enhanced performance in terms of delivery ratio and routing overhead without exploiting much, the stringent resources of WSN. Trust based routing protocols are simulated using *network simulator* for 150 and 200 nodes with different coverage areas of $300\times300m^2$ and $500\times500m^2$ by varying the malicious nodes from 5 to 40. The performance parameters such as delivery ratio, routing overhead and delay of trust based routing protocols are determined for different number of malicious nodes.

Trust based security model is incorporated in Dynamic Source Routing (DSR) protocol to anticipate Trust based Dynamic Source Routing (TDSR) protocol for avoiding the compromised nodes. Using TDSR protocol, the performance are analysed and discussed. Subsequently, Trust based Adhoc On Demand distance

Vector (TAODV) routing protocol is simulated by appending node and route trust in Adhoc On Demand distance Vector (AODV) protocol to isolate the malicious nodes and improve the network performance.

Further, Trust based Greedy Perimeter Stateless Routing (TGPSR) is propounded by including trust based security framework in the location based Greedy Perimeter Stateless Routing (GPSR) protocol to circumvent the malicious nodes. Using TGPSR protocol, the performance is also studied. To enhance the performance of WSN still further, Trust based Energy aware Greedy Perimeter Stateless Routing (TEGPSR) protocol is proposed by adopting trusted path along with minimum distance and energy level in the Energy aware Greedy Perimeter Stateless Routing (EGPSR) protocol to get rid off malevolent nodes.

To summarise, in this work various trust based routing protocols for WSN have been evaluated and is found to enhance the performance of WSN by evading the compromised nodes in the network. There can be further research to implement trust based routing protocols in heterogeneous sensor networks along with energy efficient algorithms and can be extended to different traffic services.

# ACKNOWLEDGEMENT

I am duly bound to express my deep indebtedness to my supervisor and mentor, **Dr. P. Dananjayan**, Professor, Department of Electronics and Communication Engineering, for his unflinching support, selfless motivation and contagious enthusiasm from the inception of the research to the culmination stage. It would have been insuperable to present this thesis without his unstinted support. I revere him for his edification in up bringing of this work.

I express my profound gratitude and allegiance to my Doctoral Committee members, **Dr.R.Nakeeran**, Associate Professor, Dept. of ECE, Pondicherry Engineering College and **Dr.S.Sivapragasam,** Associate Professor, Department of Physics, Pondicherry University, for their magnanimous benignity and benevolence, which has enthused me to work harder and achieve the goal. I express my ingenious, sincere requital for their motivation and lively deliberation inspite of their busy schedule.

I am grateful to **Dr.E.Srinivasan**, Professor and Head Department of Electronics and Communication Engineering for the moral support and timely help during the course of the work. I am thankful to **Dr.V.Prithviraj**, Principal, Pondicherry Engineering College and Dean Incharge, School of Engineering and Technology, Pondicherry University for his whole hearted support and permitting me to use the facilities in this college for the research work.

I express my humble gratitude to **Dr.J.A.K.Tareen**, Vice Chancellor, Pondicherry University for his motivating ideas to complete the research work at the earliest and **Dr.V.V.RavikanthKumar**, Associate Professor, Department of Physics and co-ordinator, Department of Electronics Engineering, Pondicherry University, who has been very co-operative and encouraging to finish this work. I deem it a privilege to record my sincere thanks to **Dr.V.S.K.Venkatachalapathy**, **Principal**, **Sri Manakula Vinayagar Engineering College** and also the **MANAGEMENT** of **SMVEC** for their constant support and encouragement during the period of my research work.

I am thankful to **Dr.S.Sivamurthy Reddy**, Prof. Dept. of Civil Engineering for many prolific discussions and comments in shaping my thesis work. I express my heartfelt gratitude to **Dr.L.Nithiyanandam**, Asst. Prof, **Dr.K.Jayanthi**, Asst. Prof., Dept. of ECE and **Dr.Alamelu Nachiappan**, Assoc. Prof, Dept. of EEE for their fruitful suggestions, comments and inputs in framing my thesis work. I profusely thank **Dr.Sivaradje**, Asst. Prof., Dept. of ECE and **Dr.B.Geethalakshmi,** Asst. Prof.**,** Dept. of EEE for their advice and perpetual support.

A special thanks to **Ms.Valli**, Research Scholar, Dept. of ECE for providing necessary inputs and helping me enormously during the thesis preparation and **Mrs.J.Vidhya**, Research Scholar, Dept. of ECE for her useful ideas and deliberations during the research work. I express my gratitude to **Mrs.Angayarkanni Dananjayan** for her courtesy and motivation during the course of my research work. I am thankful to my friends **Mr.P.Raja, Mr.R.Surender, Dr.V.Nagarajan** and **Dr.N.Kumarathan** for the timely help I have received from them.

I am thankful to M.Tech students **Ms.PadmaPriyadarshini** and **Mr.Pavankumar** and B.Tech students, **Mr.D.Sathian, Mr.Ragothaman and Mr.Vignesh** for the help I have received from them at different times.

I wish to deposit my deepest gratitude to my parents **Mr.Punniakodi** (Late) and **Mrs. Dhanalakshmi**, my husband **Mr.R.Muralidharan**, my son **Master.M.SaiNarendran,** my **father-in-law** and **my sisters** who have helped me, caressed me, encouraged me and motivated to complete this work.

Finally, I bow before my **Sadguru Shri, Shirdi Sai Baba** and the **Almighty** for helping me to complete this work successfully and to come out with flying colours.

**(P.SAMUNDISWARY)**

# TABLE OF CONTENTS

| CHAPTER No. | TITLE | PAGE No. |
|---|---|---|

# LIST OF FIGURES

| FIGURE No. | TITLE | PAGE No. |
|---|---|---|

| FIGURE No. | TITLE | PAGE No. |
|---|---|---|

| FIGURE No. | TITLE | PAGE No. |
|---|---|---|

| FIGURE No. | TITLE | PAGE No. |
|---|---|---|

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **AODV** | Ad hoc On Demand distance Vector |
| **ARAN** | Authenticated Routing for Ad hoc Networks |
| **ARIADNE** | A secure on demand RoutIng protocol for AD hoc NEtworks |
| **ATV** | Advertised route Trust Value |
| **CONFIDANT** | Cooperation Of Nodes, Fairness In Dynamic Ad hoc NeTworks |
| **CORE** | COllaborative REputation |
| **DoS** | Denial of Service |
| **DSDV** | Destination Sequenced Distance Vector |
| **DSN** | Destination Sequence Number |
| **DSR** | Dynamic Source Routing |
| **DTM** | Direct Trust Measure |
| **EGPSR** | Energy aware Greedy Perimeter Stateless Routing |
| **GAF** | Geographic Adaptive Fidelity |
| **GEAR** | Geographic Energy Aware Routing |
| **GPSR** | Greedy Perimeter Stateless Routing |
| **ID** | IDentification |
| **IDEA** | International Data Encryption Algorithm |
| **INSENS** | INtrusion- tolerant routing protocol for wireless SEnsor NetworkS |
| **LBKs** | Location-Based Keys |
| **LEAP** | Localised Encryption and Authentication Protocol |
| **LiSP** | Lightweight Security Protocol |
| **LKHW** | Logical Key Hierarchy for Wireless sensor networks |
| **LSec** | Light weight Security |
| **NAM** | Network AniMator |
| **OTV** | Observed Trust Value |

| | |
|---|---|
| **QID** | Query IDentifier |
| **QSEC** | Query SEquenCe |
| **RERR** | Route ERRor |
| **RREP** | Route REPly |
| **RREP-Ack** | Route REPly Acknowledgment |
| **RREQ** | Route REQuest |
| **RSA** | Rivest, Shamir and Adleman |
| **RSV** | Route Selection Value |
| **SA** | Security Association |
| **SAR** | Security Aware ad hoc Routing |
| **SEAD** | Secure Efficient Ad hoc Distance vector |
| **SECK** | Survivable and Efficient Clustered Keying |
| **SeRINS** | Secure alternate path Routing IN Sensor network |
| **SHEER** | Secure Hierarchical Energy Efficient Routing |
| **SIGF** | Secure Implicit Geographic Forwarding |
| **SKC** | Symmetric Key Cryptography |
| **SLEACH** | Secure Low Energy Adaptive Clustering Hierarchy |
| **SNEP** | Sensor Network Encryption Protocol |
| **SPAAR** | Secure Position Aided Ad hoc Routing |
| **SPIN** | Sensor Protocol for Information via Negotiation |
| **SPINE** | Secure Positioning In sensor NEtwork |
| **SRP** | Secure Routing Protocol |
| **TAODV** | Trust based Ad hoc On Demand distance Vector |
| **TDSR** | Trust based Dynamic Source Routing |
| **TEGPSR** | Trust based Energy aware Greedy Perimeter Stateless Routing |
| **TESLA** | Timed Efficient Stream Loss-tolerant Authentication |
| **TGPSR** | Trust based Greedy Perimeter Stateless Routing |
| **TIK** | TESLA with Instant Key disclosure |
| **TinySec-AE** | TinySec-Authenticated Encryption |
| **TinySec-Auth** | TinySec-Authentication |
| **TLC** | Trust Level Counter |
| **TTL** | Time To Live |

| | |
|---|---|
| **TTP** | Trusted Third Party |
| **TUI** | Trust Update Interval |
| **WSN** | Wireless Sensor Network |
| μ**TESLA** | Micro version of Timed Efficient Stream Loss-tolerant Authentication |

# LIST OF SYMBOLS

| | |
|---|---|
| $R_{id}$ | Route ID |
| $S$ | Source node |
| $D$ | Destination node |
| $i$ | Node |
| $P$ | Immediate upstream node |
| $N$ | Immediate downstream neighbour node |
| $j$ | Neighbour node |
| $n$ | Periodic interval |
| $E_{i0}$ | Initial energy of the $i^{th}$ node |
| $E_{in}$ | Energy of $i^{th}$ node at the start of the $n^{th}$ periodic interval |
| $H_p$ | HELLO period |
| $R_{in}$ | Rate of energy consumption of the $i^{th}$ node after $n^{th}$ periodic interval |
| $F_{in}$ | Fraction of energy consumption of the $i^{th}$ node after $n^{th}$ periodic interval |

# CHAPTER 1

# INTRODUCTION

## 1. 1 GENERAL

Modern communication began with the invention of “Telegraphy” by Samuel Morse and “Telephone” by Alexander Graham Bell. Today, telecommunication industry is the multibillion dollar industry connecting millions of people all over the world through public switched telephone network. Technological advancements in the field of computers have made the area of telecommunication to experience rapid development resulting in improvement in the life style. Telecommunication network supporting wireless connections used for multimedia services leads to the refinement of wireless communication networks. In the last two decades, wireless communication industry has grown by orders of magnitude, fueled by improvement in digital and RF circuit fabrication, very large scale integration techniques and other electronics technologies. Since then, the new wireless communication methods and services have been enthusiastically adopted by people [1]. Wireless communication network consists of mobile communicating devices and wireless network infrastructure. The mobile communicating devices are equipped with wireless front-ends to communicate with the wired backbone through the wireless network infrastructure. A collection of switches and wireless transceivers form the wireless network infrastructure used to interconnect several of the mobile communicating terminals.

In general, wireless network has two types of topologies. They are infrastructure or centralized topology and adhoc or distributed topology [2]. The first paradigm has fixed infrastructure that supports communication either between mobile terminals or between mobile and fixed terminals through access points. These networks are designed for large coverage areas with multiple access points. Cellular topology is the dominant technology used in all large scale terrestrial and satellite wireless networks due to less co-channel interference. The major snag is the

difficulty in handoff from one access point to another access point without noticeable delay.

The second paradigm is adhoc network which is an infrastructureless network. This network is self-configuring and adapts to changes in the topology. The adhoc topology is suitable for rapid deployment of a wireless network in a mobile environment. Moreover, the adhoc network can be either constructed or destructed quickly and autonomously. The adhoc network consists of wireless mobile nodes having ability to communicate with each other without any central base station. The nodes can be both hosts (laptops or PDA) and routers equipped with high speed processor [3]. Each node can directly converse with other nodes within its transmission range. This network has smaller transmission range compared to that of cellular system. Even though the network supports scalability, mobility and adaptability to the topology changes, node localization and guaranteed network performance is a challenging task when nodes with sensing capability are deployed randomly in hostile environment. Wireless Sensor Network (WSN) has been considered as an incarnation of mobile adhoc network for such environment.

The advances in miniaturisation techniques and wireless technologies have contributed to the fabulous growth of wireless sensor network [4]. The features of sensor network are dense deployment of nodes, decentralization and frequently changing topology due to fading and node failures. Sensor network is also capable of self-organising without requiring the existence of a supporting infrastructure. The infrastructure of wireless sensor network can be divided into two parts, the data acquisition network and data dissemination network [5]. The data acquisition network contains sensor nodes and data sink. On the other hand, data dissemination network interfaces the data acquisition networks to the users and is a collection of wired or wireless networks.

Recently, WSN has drawn a lot of attention due to broad applications in military and civilian operations such as weather monitoring, wildlife monitoring and disaster management. In such applications, enormous

numbers of sensor nodes are to be scattered randomly in a dangerous and unsupervised environment which makes the network prone to a variety of potential attacks. Hence, security is one the major challenges faced by sensor network in today's scenario to enhance the performance of the network.

### 1.1.1 Wireless Sensor Network

Sensor network consists of hundreds to thousands of small, low cost multifunctional sensors powered by low-energy batteries [6]. Each sensor node comprises of sensing, processing, transceiver, mobiliser, position finding system and power units. Sensor nodes deployed in strategic areas sense the changes in their surroundings and send these changes to a data sink. The data sink may be a fixed or mobile node capable of connecting the sensor network to wireless network infrastructure or internet to access the reported data.

The potential of collaboration among sensors in data gathering, processing and monitoring applications require novel routing techniques. Hence, routing of data from sensor node to data sink is a very challenging task in sensor networks that distinguish them from contemporary communication and wireless adhoc networks. It is not possible to build a global addressing scheme for the dense deployment of sensor nodes as the overhead of identity maintenance is high. Also in contrast to typical communication networks, almost all applications of sensor networks require the flow of sensed data from multiple regions (sources) to a particular sink. Further, generated data traffic has significant redundancy, since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization. Further more, sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage.

In view of the aforesaid constraints, many routing techniques have been proposed for wireless sensor network by considering the inherent features along with the applications and architecture requirements of sensor networks [7]. The routing protocols can be classified into three categories, namely, proactive, reactive and

hybrid protocols depending on how the source finds a route to the destination. In proactive protocols, all routes are computed before they are really needed. However, routes are computed on demand in reactive protocols. Hybrid protocols use a combination of these two protocols. Destination Sequenced Distance Vector (DSDV) is the representative example of the proactive protocol. Dynamic Source Routing (DSR) and Adhoc On Demand distance Vector (AODV) routing are the reactive routing protocols. It is preferable to have reactive routing protocols rather than table-driven routing protocols for dynamic sensor nodes.

Further, the routing techniques are classified into three categories based on the underlying network structure such as data-centric, hierarchical, and location based routing. Data-centric protocols are query-based and depend on the naming of the desired data. Direct diffusion is an example of data centric protocol. Hierarchical protocols aim at clustering the nodes, so that, cluster heads can do some aggregation in order to decrease the amount of transmission of data to save energy. The intend of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication within a particular cluster. Low Energy Adaptive Clustering Hierarchy (LEACH) is one of the cluster based routing protocols. Location based protocols utilize the position information of the mobile nodes to transmit the data to the desired regions rather than the whole network. Location based protocols are also called as position based or geographic routing protocols. Greedy Perimeter Stateless Routing (GPSR), Geographic Adaptive Fidelity (GAF) and Geographic Energy Aware Routing (GEAR) are some of the location based routing protocols.

However, the routing protocols of sensor networks are exposed to various attackers when sensor nodes are randomly distributed in an unattended environment. The performance of routing protocols in terms of forwarding rate, control packets and latency will be degraded in the presence of malevolent nodes. Hence, the network with security schemes is required to improve the performance of the system.

## 1.2 SIGNIFICANCE OF SECURITY SCHEME IN WIRELESS SENSOR NETWORK

The wireless networks such as ad hoc and sensor networks are more vulnerable to security threats than wired networks, as the transmission medium is wireless type in such networks. In addition, sensor networks are also susceptible to variety of attacks due to resource constraints and random deployment of nodes in insecure environment [8]. Hence the adversary can easily capture, compromise and hijack the nodes of the sensor network. They can disrupt the network by joining either internally or externally with the help of hijacked nodes. The attacks launched by internally generated compromised nodes are the most dangerous type of attacks. These compromised nodes can also carry out both passive and active attacks in the network. In passive attack, a malicious node only eavesdrops upon the packet contents and traffic flow patterns. However, active attacks may imitate and drop or modify legitimate packets.

The different types of passive attacks are eavesdropping in the physical layer and collision in the data link layer. Jamming and Denial of Service (DoS) attacks [9, 10] are some of the active attacks in the physical and data link layer. The various active attacks of the network layer are spoofed and replayed routing information attack, selective forwarding attack, blackhole/sinkhole attack, sybil attack, wormhole attack and HELLO flood attacks [11]. These active attacks will corrupt the packet and modify the routing information and compromise the entire network. But providing security against these attacks is a crucial issue in sensor networks.

The security mechanisms devised for traditional wired networks to detect and eradicate the various attacks are not applicable to sensor network because of its limited energy, small memory size, low bandwidth and more number of nodes. However, spread spectrum techniques and error correcting codes are used to mitigate the effect of external attacks such as jamming in the physical and collision in the data link layer [12-14]. In addition, the encryption and decryption

mechanisms [15-20] are the security schemes used to defend against the external attacks of physical and data link layer. Moreover, security mechanisms using cryptographic methods are not used to get rid of the network from internally generated compromised nodes.

Further, security of sensor network can be enhanced by implementing an efficient key management scheme [21-23] in the link layer to safeguard the network from internal attacks of data link layer and network layer. The shared keys used in this scheme will be compromised. The secured key management schemes also require centralized or distributed key repository systems resulting in more overhead. The same could not be provided by sensor network due to its meager resources.

Therefore, the existing security mechanisms [24] such as link layer encryption schemes, secured communication protocols and identity verification with cryptographic hash functions are used to preserve the network from external attacks of data link layer and some of the external attacks such as sybil attack and HELLO flood attack of network layer. However, these are only the first approximations for defense against the attacks from the outsider. Even though, number of approaches has been done in key distribution and management scheme to defend against internal attacks, these schemes do not provide less communication overhead for sensor network with high scalability.

Moreover, any security solution with a static configuration may not be suitable for ad hoc networks because nodes have mobility and the network topology may change frequently. Nodes have to detect the possible attackers because their neighbours are not fixed. Similarly, for a sensor network, a malicious node with mobility can roam and attack different parts of the network. Further, other legitimate nodes will be claimed to be illegal by the attackers. In addition, an attacker can frequently flood fake or dummy messages to exhaust other nodes energies because nodes of sensor networks normally rely on batteries to provide energy. The adversary also disguises its packet as normal ones or replays other nodes' packets to waste energy of normal nodes.

Further more, most routing protocols of sensor networks do not include security considerations at the design stage. Therefore, attackers can easily launch various active attacks by exploiting security holes in the protocols after the deployment of nodes in an uncontrolled environment. Hence, it is essential to evade the active attacks by integrating security algorithms in routing protocols in order to achieve performance improvement in sensor networks.

## 1.3 SCOPE OF THE WORK

The present wireless network requirement is to transmit the data from the sensor node to base station in a secured path and achieve high network performance against the attacks of the various layers. The search to fulfill this requirement is achieved by implementing security mechanisms in the different layers to protect the network from variety of attackers.

Various public key cryptography techniques are developed to provide security services such as encryption and authentication in link layer to shield the sensor network from external attacks. However, asymmetric key cryptography scheme needs complicated computation, high energy and large memory space which cannot be performed on sensor networks. This scheme also has no provision to alleviate internal attacks created by malicious nodes.

Subsequently, several symmetric key cryptography mechanisms are explored to protect the network from link layer attacks in order to overcome the above constraints such as computation and energy consumption. In this scheme, unique symmetric keys are assigned to each node before the deployment of the network. These symmetric keys are shared by the nodes with the base station. However, this cryptographic technique involves a significant overhead for storing hundreds of bytes of keys generated. The other drawback with this approach is that it is not resistant against node capture attacks in which an adversary can pollute the entire sensor network by compromising only one single node.

Further, communication protocol such as Sensor Protocols for Information via Negotiation (SPIN) [25] is developed to achieve confidentiality, integrity and authentication. SPIN is based on symmetric key mechanism. Hence, this scheme increases communication overhead and buffering requirements. Moreover, SPIN does not completely deal with malicious nodes.

TinySec [26] is another communication protocol developed by implementing link layer encryption in TinyOS beaconing protocol. TinySec provides message integrity and authentication by using message authentication code. TinySec reduces overhead, latency and memory size. However, this scheme is not fully resistant against node capture attack created by compromised nodes.

Subsequently, secure key management techniques [27-38] are implemented in the link layer to safeguard the network from internal attacks. Key management generally addresses key establishment, key maintenance and key revocation. Key establishment is achieved through either the use of public key or symmetric keys. However, public key protocols are not suitable for sensor networks because they utilize asymmetric keying. This involves the maintenance of two different keys namely encryption and decryption keys. The encryption key is made public, while the decryption is private. The problem with this technique is that it is too computationally intensive for large number of sensor nodes. The other drawback of this method is the obligation of large memory capacity for storage of asymmetric keys. Therefore, symmetric key management scheme is the alternative technique to shield the network from active internal attacks. The main shortcoming of symmetric key protocols is the potentially insecure key exchange.

Another, a new type of key management technique, namely deterministic or random key pre-distribution scheme [39-42] is used to improve the resilience to internal attacks for large sensor networks. In this scheme, a set of keys is deterministically or randomly selected and stored from a pool of network keys. Any two nodes, which are able to find a common key within their respective subset of keys, are able to establish communication and mutual authentication via symmetric

shared key cryptography. The major snag with this mechanism is the requirement of large memory for the nodes which limits the scalability of such schemes. Also, due to the probabilistic nature of the key subset selection, communication between any given pair of nodes is not guaranteed.

Further more, a key management scheme considering different type of key establishment schemes such as symmetric key, pair wise key and hash function used in Localized Encryption and Authentication Protocol (LEAP) is developed for hierarchical WSNs to evade the attacks of network layer such as sybil attacks. This scheme provides confidentiality, authentication and freshness [43]. The problem with this scheme is that the entire network is polluted if the master key is compromised. Also it requires large overhead which is not provided by resource limited sensor network.

Also, the intrusion detection scheme, namely, INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) is implemented in the remote data sink for sensor networks to protect the network from active attacks of network layer [44]. The intrusion detection schemes construct forwarding tables at each node to facilitate the communication between sensor nodes and a data sink. However, this will drastically increase traffic between sensor nodes and remote sink. The other limitation of INSENS is that it increases computation and storage requirements at the data sink.

Secure Implicit Geographic Forwarding (SIGF) is a configurable protocol family for secure routing in sensor networks [45]. This secure routing protocol provides a configurable security framework for location based routing of sensor networks. SIGF mitigates selective forwarding as well as black hole attacks. The main problem in SIGF is the lack of source authentication. Hence, SIGF reduces the network lifetime by increasing the network end to end delay.

Secure diffusion [46] is the secured variant of direct diffusion routing protocol [47] that uses location-binding symmetric keys instead of traditional

symmetric keys bound for the identification of sensor nodes. The secured routing protocol enhances the performance of diffusion in the presence of internally generated compromised nodes. Location binding keys are used by sink to authenticate the received sensing data and sensor nodes use pair-wise neighbour keys to establish secure gradients between the nodes. The drawback is that location binding keys for large number of nodes increases the management cost at the base station.

Further more, a Secure alternate path Routing IN Sensor networks (SeRINS) is developed by using neighbour report system [48]. SeRINS remain resilient in the presence of malicious nodes which launch selective forwarding attacks in the network. This scheme is robust by excluding the compromised nodes which inject inconsistent routing information from the network.

It is clear that the aforesaid secured routing algorithms are confined to limited size of sensor network having nodes with static configuration. Moreover, these secured routing protocols require more computation and memory. Also, it is evident that more trust has been focused on resilience against node capture rather than the performance enhancement of the network. Hence, an attempt has been made in the present work to incorporate trusted security frame work in various routing protocols to identify and isolate the active attacks to achieve better performance in large size sensor network having dynamic nodes.

## 1.4 OBJECTIVE

An attempt has been made in the present work to improve the network performance of WSN through various secured routing protocols by employing trust based security algorithm in the routing protocols.

- To evaluate the performance of sensor network in terms of delivery ratio, delay and routing overhead by adopting the proposed Trust based Dynamic Source Routing (TDSR) protocol incorporating trust frame work in the DSR protocol to get rid of malicious nodes.

- To examine the performance of sensor network incorporated with Trust based Adhoc On Demand Distance Vector (TAODV) routing protocol by using node and route trust based routing decisions in the AODV protocol.
- To study the efficiency of the proposed Trust based Greedy Perimeter Stateless Routing (TGPSR) against the malicious nodes by including trust based security model in GPSR and subsequent effect on the performance metrics of sensor networks.
- To analyse the system performance in terms of routing overhead, delivery ratio and delay by appending security mechanism using trust based routing decisions in Energy aware Greedy Perimeter Stateless Routing (EGPSR).

## 1.5 ORGANISATION OF THESIS

Chapter 1 outlines an overview of WSN. The various security techniques used in sensor network against attacks are also described. The significance, scope of the work, objectives of the work and organization of the thesis are also presented in this chapter.

An elaborate review of literature related to the different types of security mechanisms against various attacks in wireless sensor network is presented in Chapter 2. The summary of the literature justifying the present work is also furnished at the end of chapter.

Chapter 3 deals with the trust based security framework imposed in DSR protocol to circumvent the sinkhole attack in the network. Performance analysis is also discussed with the help of simulation results to prove the efficiency of the proposed model.

The performance improvement of the sensor network by employing trust levels in AODV routing protocol to elude the malicious nodes in the network is

presented in Chapter 4. Further, the simulation results and discussion on the performance of network are incorporated in this chapter.

Chapter 5 highlights the security enhancement of sensor network by deploying trust based security model in GPSR in the presence of compromised nodes. The simulation results with a detailed discussion on the effect of trust based mechanism on security enhancement of sensor network are also presented in this chapter.

The security technique using trust model in the EGPSR to avoid the threats in wireless sensor network are dealt in Chapter 6. Finally, the performance analysis of the proposed protocol with the assistance of simulation results is presented.

In Chapter 7 the thesis is concluded by emphasizing the major conjecture of the present work. A summary of research contribution and the scope for future studies are also included in this chapter.

# CHAPTER 2

# LITERATURE SURVEY

## 2.1 GENERAL

The extensive literature collected related to performance enhancement of security mechanism against various attacks exposed by WSN using link layer encryption, authentication broadcast and key management schemes is critically reviewed and presented in this chapter. A comprehensive review of literature on the evolution of various secure routing protocols for adhoc and sensor networks and their performance is also presented. Further the summary of review of literature is furnished at the end of the review to substantiate the scope of present work.

## 2.2 REVIEW OF LITERATURE

Jamal.N. Al-karaki and Ahmed E.Kamal [7] highlighted the design challenges of routing protocols of WSN. A comprehensive review has been presented on application and architecture based routing techniques. Subsequently, Karlof and Wager [8] brought out the various security issues in WSNs. Various security threats have been highlighted and counter measures have been proposed against various attacks existing in the different layers of networks. It has been emphasized that routing protocols should be designed with security in mind.

Perrig *et al.* [9] outlined the variety of attacks including node capture, physical tampering and DoS attacks. Also, the state of security mechanisms such as secrecy, authentication, key establishment and robustness to DoS attacks in sensor networks has been highlighted. These aspects have been fulfilled by incorporating high level security services. Also, scope of future research in the area of WSNs has been highlighted.

Wang *et al*. [10] discussed about the security requirements, constraints and attacks with their corresponding countermeasures in WSNs. Various security protocols of WSNs have been highlighted with the merits and demerits. It has been concluded with the possible research directions on security in WSNs. Al-Sakib Khan Pathan *et al*. [11] examined the security related issues and challenges in WSNs. The different types of security threats and various security mechanisms against these threats are also analysed. It has been highlighted that holistic approach of security schemes should be developed for ensuring layered and robust security in WSNs.

Jones *et al.* [12] addressed a holistic security model involving a frequency hopping scheme to defend against the jamming attacks in the physical layer. This scheme provides secure paths rather than securing each link between sender and receiver. Although, the proposed method reduces the effect of jamming, DoS attacks are still exist. DoS attacks affect the entire network, as there is no mechanism to detect and or isolate the compromised segments of the network.

Wenyuan Xu *et al.* [13] highlighted about the different type of jamming attacks employed against sensor network. These jamming attacks are accomplished by an adversary by either bypassing medium access layer protocols or emitting a radio signal targeted at jamming a particular channel. Two different approaches have been proposed to secure sensor network from jamming attacks. The first approach is to simply retreat from the interferer consummated by either spectral evasion or spatial evasion. On the other hand, the second approach is to compete more actively with the interferer by adjusting resources such as power levels and communication coding in order to achieve communication in the presence of jamming attacks. However, these two approaches have not addressed the other DoS attacks and their defense measures with respect to physical, data link and network layer.

Wood and Stankoviv [14] presented a comprehensive assessment of various DoS attacks and their counter measures and methodologies to apply in sensor networks. These attacks are presented based on the security vulnerability of the physical, data link, network layer and transport layer. An attempt has been made

to reinforce the need for wireless sensor network security protocols that are robust to DoS attacks. Finally, it has been concluded that security considerations must be contemplated and incorporated at the design stage of protocol, but not after implementation.

Wander *et al.* [15] developed public key cryptographic techniques used to protect the network from various medium access layer attacks. In this regard, Brown *et al*. [16] found that public key algorithms such as Rivest, Shamir and Adleman (RSA) usually require in the order of tens of seconds and upto minutes to perform encryption and decryption operations in constrained wireless sensor devices vulnerable to DoS attacks. Further, Carman *et al*. [17] pointed out that public key schemes usually take thousands of nanojoules to do simple multiply function by using microprocessor. In contrast, Symmetric Key Cryptography (SKC) algorithms and hash functions consume less computational energy than public key algorithms. SKC algorithms [18] provide confidentiality, integrity and authentication type of security services to sensor networks. These algorithms are simple and easy to implement in resource-constrained devices. The suitability of SKC primitives on sensor nodes was analysed mainly by Ganesan *et al*. Also, the feasibility of the software implementations of SKC algorithms such as RC4, skipjack, International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) have been evaluated. It has been concluded that the most effective algorithms such as RC4 and skipjack exhibited 10% lesser communication overhead than AES algorithms. Further, an attempt has also been made to utilise cryptographic hash functions to compress a set of data of variable length into a set of bits of fixed length. Hash functions are usually used for assuring the integrity of the information. However, hash functions are around ten times slower than SKC algorithms.

Slijepcevic *et al.* [19] proposed a security scheme with secure communication on three levels. Level 1 is reserved for the most sensitive information collected by sensor. Level 2 is for the location information conveyed in messages and level 3 is meant for application specific information. This scheme is used based on the assumption that sensor nodes have access to the content of any message. However, authenticity and integrity of data are not addressed in this scheme.

Chen *et al*. [20] attempted to evaluate two security protocols. An efficient shared-key algorithm like RC5 is used in the first protocol to guarantee confidentiality and authentication of information transmitted from the base station to node. In the second protocol, a hash function similar to that used by Timed Efficient Stream Loss-tolerant Authentication (TESLA) is used to achieve node authentication. Conversely, this scheme does not deal with DoS attacks.

Perrig *et al*. [25] proposed SPIN for link layer security in sensor networks. The two building blocks for these suites are Sensor Network Encryption Protocol (SNEP) and a Micro version of Timed Efficient Streamed Loss-tolerant Authentication (μTESLA). The SNEP is used to provide confidentiality, data integrity and freshness. The μTESLA provides an authenticated broadcast. Also, two applications have been proposed for their protocols. An authenticated routing was explored in the first case and the other uses symmetric cryptography to set up node-to-node key agreement using the base station as a trusted agent. One of the main shortcomings of this scheme is that no provision is made to mitigate internal attacks, DoS attacks and network traffic analysis attacks. Also, the proposed scheme increases the latency, complexity of computation and buffering requirements. Furthermore, the static network topology is assumed by ignoring the mobile nature of sensor nodes.

Karlof *et al*. [26] presented TinySec, link layer security architecture for sensor network which is faster than SPIN. TinySec has supported two different security options such as authenticated encryption (TinySec-AE) and authentication (TinySec-Auth). The data payload is encrypted with authenticated encryption mode and the packet is authenticated by using message authenticated code. In authentication mode, the entire packet alone is authenticated with the message authenticated code but the data payload is not encrypted. This technique is assumed to have a global common secret key among the nodes (which is assigned before the deployment of the network) to provide security services such as encryption and authentication in link layer. However, the proposed approach is not resistant against node capture attacks in which an attacker can disrupt the entire sensor network by

corrupting the message authenticated code of the packet transmitted by the node. Also, it limits the number of nodes of the network as it requires additional memory size of 104 bytes for storing single key.

Link layer encryption using asymmetric and symmetric key cryptographic techniques, authentication broadcasts and identity verification along with the cryptographic hash functions proposed by various researchers are used to protect the network from the outside attackers. However, the aforementioned security mechanisms are only the first approximations to defend against the attacks from the outsider.

Subsequently, secure key management mechanism [27, 28] is developed to establish secure communication in WSNs by circumventing internal attacks. Key management scheme [21-24] consists of four phases. The first phase is key-distribution phase where secret keys are distributed to sensor nodes to use with the security mechanisms. This phase is also called as key set up phase. The second phase is the shared-key discovery phase which starts after the sensor network deployment. Each sensor node discovers its neighbours and shares a common key with each of them. Key establishment phase is the third phase where each pair of neighbouring keys which do not have common keys, establish one or more keys. Key establishment between two nodes is achieved by using pre-distributed keys and exchanging messages directly over their insecure wireless link or over one or more secure paths on which each link is secured with a secret key. However, sensor nodes are prone to variety of attacks including node capture which leads to limited lifetime of the network. Also, security materials on existing ones are to be updated when new nodes are deployed. The fourth phase is the key update phase where the secret keys are to be updated to secure the links between neighbouring nodes.

Further, three classes of key management such as key distribution, key agreement and key pre-distribution schemes [29, 30] have been proposed. Key distribution scheme relies on Trusted Third Party (TTP) to distribute session keys to nodes. These schemes are impractical to implement in sensor networks because TTP

may not be available to some of the nodes due to communication range limitations, node movements and unknown topology prior to deployments. The second class is a key agreement scheme which is a self enforcing scheme in which each node takes part in establishing a shared secret key through mutual exchanged messages among the nodes in a secure manner. These protocols are almost fully distributed or self organized without the need of TTP. However, these protocols are not still feasible in sensor networks for the following reasons. The schemes are not robust to variable topology or intermittent links frequently occurring in sensor networks. In addition, all nodes need to be alive before the key agreement process is over. If any node leaves in the midst due to battery outage, the remaining nodes need to re-run the process from scratch. Evidently, these requirements could not be satisfied in wireless sensor networks.

Also, a key agreement scheme [31-36] which depends on asymmetric cryptography is not computationally efficient for more sensor nodes. More so, the obligation of large memory capacity for storage of asymmetric keys makes such public-key cryptography operations impractical. Hence, key agreement scheme using symmetric keys is the preferred technique to shelter the network from internal active attacks. The symmetric keying protocols use two shared keys for encryption and decryption. The major drawback of symmetric key protocols is the potentially insecure key exchange. The problem arises because the two communicating nodes must know the shared key prior to the commencement of communication. Therefore, the problem is the inability of the nodes to ensure that the shared keys have not been compromised.

Key pre-distribution scheme is the third class of key management scheme where key information is distributed among all sensor nodes prior to deployment. Eventhough, key pre-distribution scheme offers practical and efficient solutions to the key management problem in sensor network; nodes are not likely to stay in the same neighbourhood as they were prior to deployment. Hence, knowing the set of neighbours deterministically might not be feasible due to the randomness of deployment. Moreover, adding new nodes to a pre-existing sensor network is

difficult because the existing nodes do not have the new nodes' keys. In addition, it does not exhibit desirable network resilience, if the newly entered node is compromised node. Hence, the entire network will be compromised. Further, there are several approaches developed by various researchers based on key pre-distribution and key establishment scheme in key management mechanism.

Subsequently, Blom [37] proposed deterministic key pre-distribution method which allows any pair of nodes in network to find a pair-wise secret key which is created by the base station. This scheme provides secure communication for uncompromised nodes until node is compromised. Later, Blundo *et al.* [38] developed a polynomial based deterministic scheme for group key pre-distribution. This scheme is resistant against compromised node upto a certain degree of polynomial based shared key and require less overhead. However, the storage cost for polynomial share is exponentially increased with group size, making it prohibitive in sensor network with low memory capacity.

Later, Eschenauer and Gligor [39] proposed a random key pre-distribution scheme where each sensor node receives a random subset of keys from a large key pool before deployment. This scheme is addressed by key distribution, revocation, re-keying and resilience to senor node capture issue. Key distribution involves three phases such as key pre-distribution, shared-key discovery and path key establishment. The next step in this scheme is revocation to eliminate the key ring of compromised nodes. Re-keying is described as self-revocation of a key by an expired node. The last step is resilience in which an adversary injecting fake data or capturing the sensor node is detected. However, the proposed scheme requires more memory for increased nodes.

Subsequently, Chan *et al*. [40] extended the idea of Eschenauer by presenting three new key establishment mechanisms in key pre-distribution schemes such as a q-composite scheme, multipath reinforcement and a random-pair-wise key scheme. Also, probabilistically establishing pair-wise keys between neighbouring nodes have been proposed to achieve secure communication. In this approach, a

random subset of keys from a key pool is pre-assigned to every node. Any two nodes establish a pair-wise key based on the subset of shared key between them. Though, this security framework is flexible, most of the key pre-distribution schemes rely on sensor nodes to broadcast a large number of pre-loaded keys identities to find pair-wise keys between neighbouring nodes. This leads to a huge communication overhead. In addition, memory availability may decrease as each node has to store several hundred keys.

Further, Pierto *et al.* [41] proposed a probabilistic model to refine Eschenauer *et al*'s basic scheme. The model was developed by using random key management assignment. Two protocols such as direct and cooperative are used to establish secure pair-wise communication between sensors by assigning a small set of random keys to each sensor. The idea is later converged into the pseudo random generation of keys having more energy efficiency than the key management schemes proposed earlier.

Liu and Ning [42] introduced a general framework for establishing pair-wise keys between sensors on the basis of a polynomial based key pre-distribution protocol. Later, two instantaneous security frameworks such as a random subset assignment key pre-distribution scheme and a hypercube-based key pre-distribution scheme are presented. Finally, a suitable technique has been proposed to reduce the computation at the sensors so as to implement the scheme efficiently.

Subsequently, Du *et al*. [49] proposed pair-wise key pre-distribution to improve the resilience of the network by lowering the initial payoff of smaller scale network attacks thus forcing the adversary to attack at larger scaled to compromise the network. Further, Du *et al* [50] presented a key scheme based on deployment knowledge. The proposed key management scheme takes advantage of the deployment knowledge where the sensor's position is known to prior deployment. It is not feasible to know the exact location of neighbours because of the randomness of the deployment, but it is realistic to know the set of likely neighbours.

Furthermore, Zhu *et al.* [43] propounded a pair-wise key management scheme, namely, LEAP for hierarchical sensor network. LEAP use a network-wise master key to establish a dedicated pair-wise key between each pair of neighbouring sensor nodes. Also, LEAP supports the establishment of four types of keys for each sensor node such as an individual key shared with the data sink, a pairwise key shared with another sensor node, a cluster key shared with multiple neighbouring nodes and a group key that is shared by all the nodes in the network. Hence, LEAP offers multiple keying mechanisms required for different types of messages exchanged between sensor nodes having different security requirements. This security protocol restricts the security impact of a node compromise to the immediate neighbourhood of the compromised node. However, it is possible to compromise all pair-wise keys generated by LEAP algorithm, once the master key is compromised.

Subsequently, Pietro *et al*. [51] proposed another key management approach, namely, Logical Key Hierarchy for Wireless (LKHW) sensor networks. Logical key hierarchy is built on top of directed diffusion which is a data centric routing protocol. LKHW is a secure multicast scheme that enforces backward and forward secrecy. LKHW uses a hierarchy or tree structure to store keys. The root of the tree serves as the key distribution center and each leaf represents a user. Each node stores the set of keys belonging to its direct ancestors up to the key distribution centre. The reason for using hierarchy is to increase efficiency of re-keying. The main snag in the proposed scheme is the increment of energy consumption due to more number of re-keying mechanisms for increased number of nodes.

Later, Eltoweissy *et al*. [52] suggested exclusion basis system based group key management scheme for hierarchical network. In this scheme, an arbitrary subset of clone sets in the network is organized into secure communication groups. This group key management scheme performs a number of functions such as session key initialization to establish secure link group, session key revocation to revoke the most recent session key and re-keying the key after detecting the node compromise. However, the communication cost of this scheme increases with the network node

density and also with the parameters of key pre-distribution scheme used in group key management. Hence, the communication overhead is also increased.

Further, Chorzempa *et al.* [53] presented Survivable and Efficient Clustered Keying (SECK), appropriate for large scale sensor network with a multi-tier hierarchical structure deployed in a hostile environment. SECK is a key management scheme, which includes location training scheme for establishing and updating administrative keys, and a scheme distributing session's keys using administrative keys. SECK is able to efficiently refresh keys, revoke captured nodes and efficiently reestablish secure group communications after node captures are detected. Although, this scheme provides low communication overhead, the memory requirement is large for storing different types of keys used in this scheme.

Further more, Zhang *et al.* [54] proposed Location-Based Keys (LBKs) correspond to the nodes' unique geographic location. In LBKs, each node obtains its unique geographic location information from the mobile robot having more powerful computation and communication capability than the ordinary nodes. Location based node-to-node authentication is achieved by facilitating the establishment of pair-wise keys between neighbour nodes in LBKs. The proposed scheme is also used to localize the impact of compromised node within their vicinity. LBKs have perfect resilience against node compromise by providing low storage overhead and good scalability. However, this scheme provides efficient counter measures against only few notorious attacks of sensor network routing protocols.

It is evident that several attempts have been made by researchers to optimize and improve the key distribution and management. However, the outcome of the research is yet to offer effective technology with higher scalability, higher network resilience, improved random key pre-distribution, lesser memory demands and lesser communication overhead.

Marti *et al.* [55] pioneered the idea of watchdog and path-rater mechanisms. In this mechanism, every node implementing the watchdog is operated in promiscuous node, which constantly monitors the packet forwarding activities of its neighbours. Also, the node using the path rater, rates the transmission reliability of all alternative routes to a particular destination node according to the reports of the watchdog. Path-rater is used to detect and mitigate routing behaviour, whereas, watchdog detects a misbehaving node. However, weakness such as ambiguous collisions, limited transmission power, false behaviour and collisions make this technique less effective.

Subsequently, Buchegger and Boudec [56] proposed Cooperation Of Nodes, Fairness In Dynamic Adhoc NeTworks (CONFIDANT). The trust manager and reputation system blocks are additionally included in watch dog and path-rater scheme in the proposed scheme. The trust manager evaluates the events reported by the watchdog and issues alarms to warn other nodes regarding malicious nodes. The alarm recipients are maintained in a friends-list which is configured through a user-to-user authentication scheme. Pretty good privacy is employed to verify the source of alarms. The reputation system maintains a black-list of nodes for each node and shares them with nodes in the friends-list. The CONFIDANT protocol is a punishment based scheme by not forwarding packets of nodes whose trust level drops below the threshold even if the node is benevolent one.

Later, Michiardi and Malve [57] proposed a COllaborative REputation (CORE) to achieve secure communication. CORE employs a complicated reputation exchange mechanism. CORE divides the reputation of a node into three components. Subjective reputation is done through observations, whereas, indirect reputation is positive report by another node. The third method is functional reputation, based on behaviour monitored during a specific task. These reputations are based on combined reputation value. This combined reputation value is used to make decisions regarding the inclusion or isolation of another node. CORE makes use of two types of entities such as a requestor and one or more providers to support a collaborative reputation mechanism. The requestor asks the providers for reputation

values and validates the obtained results with the expected results that have been derived using watchdog. However, CORE employs the measure of forwarding mechanism which is not adequate for trust computation and vulnerable to deception.

Karvets *et al*. [58] propounded a secured adhoc on demand distance vector routing protocol, namely, Security Aware adhoc Routing (SAR) for wireless networks. SAR integrates the trust level of a node and the security attributes of a route to provide an integrated security metric for the requested route from source node. The route discovery is done by quantifiable secure routes by incorporating a quality of protection as routing metric. Threats such as interception and subversion can be prevented by trust level key authentication. Replay, modification and fabrication attacks can be stopped by verifying the digital signature of the transmitted packets. One of the main drawbacks of SAR is the requirement of excessive encrypting and decryption computation at each hop during route discovery.

Authenticated Routing for Adhoc Networks (ARAN) is to provide secure communication designed in managed open environments [59]. Nodes in a managed-open environment exchange initialisation parameters before the start of communication. Symmetric session keys are exchanged or distributed through a trusted third party like a certification authority. Each node in ARAN receives a certificate after authenticating its identity to a trusted certificate server. Nodes use these certificates to authenticate themselves to other nodes during the exchange of routing messages. ARAN is efficient in discovering and maintaining routes in spite of the large overall routing overload. However, ARAN has high cost route discovery due to heavy computation.

Carter and Yasinac [60] introduced Secure Position Aided Adhoc Routing (SPAAR). SPAAR uses position information to reduce the overhead of the route discovery. In SPAAR, location is used to help in securing routing. Symmetric and asymmetric cryptography techniques are employed to encrypt route request. The two main components such as neighbour table and route table are included in the

SPAAR approach. The neigbour table needs neighbour discovery and neighbour table maintenance. Route discovery and route table maintenance are required for route table method. SPAAR encrypts location information twice by destination public key initially and then by the group key among intermediate nodes. Though, confidentiality is ensured within ad hoc networks by using SPAAR, it requires extra memory for storing routing pairs of each node and heavy processing overhead for encryption.

Yih-Chun Hu *et al.* [61] introduced secured proactive routing protocol for ad hoc networks, namely Secure Efficient Adhoc Distance vector (SEAD). In the proposed scheme, security algorithm is appended in DSDV [62]. An efficient one way hash function is used in SEAD protocol. In addition to the sequence number, next hop and destination metric of DSDV protocol, a hash value is added to each routing table of a node in order to authenticate route update. SEAD is robust against attackers by trying to create routing state in other node by modifying the sequence number of the routing metric. However, SEAD does not provide a way to prevent the attacker from tampering next hop or destination field in a routing update. Also, it does not afford a solution to protect the network from the attacker in using the same metric and sequence number learned from some recent update message for sending a new routing update to a different destination. Moreover, SEAD increases the path overhead due to the increased number of routing advertisements and size of each advertisement by the addition of hash value on each entry.

Consequentially, Yih-Chun Hu *et al.* [63] developed on demand secured routing protocol, namely, A secure on demand RoutIng protocol for ADhoc NEtworks (ARIADNE) by incorporating an efficient symmetric key cryptographic algorithms in dynamic source routing protocol to reduce the higher path overhead provided by SEAD. ARIDANE also relies on TESLA, broadcast authentication protocol for secure authentication of a routing message. ARIDANE prevents the attackers from tampering uncompromised routes consisting of uncompromised nodes. This secured on demand routing protocol is also immune to wormhole attack. However, it is still vulnerable to selfish node attacks.

Papadimitratos and Haas [64] presented Secure Routing Protocol (SRP), another secured protocol that can be applied to many of the on demand routing protocols. SRP defends against attacks that disrupt the route discovery and guarantees to identify the correct topological information. The basic idea of SRP is to set up a Security Association (SA) between a source and destination node without the need of cryptographic validation of the data by the intermediate nodes. SA is achieved through a shared key between the source and target which is done priori to the route initiation phase. The SRP uses an additional header called SRP header to the underlying routing protocols. SRP header contains the fields such as the Query SequenCe (QSEC) number, Query IDentifier (QID) number and 96 bit message authentication code field. If message authentication code field of the source matches with the message authentication code field of the destination, then authenticity of the sender and integrity of the request are verified. On reception of a route reply, source checks the source address, destination address, QID and QSEC. In case of match, source compares IP source route's reply with the exact reverse of the route carried in reply packet. If two routes also match, then source calculates the MAC field. Then the validation is successful if the two MAC are matched and SRP confirms that the reply came from the correct destination. However, SRP suffers from lack of validation mechanism for route maintenance messages as this scheme does not stop a malicious node from harming the routes to which the node already belongs to. Moreover, SRP is prone to wormhole attack, although, it is immune to spoofing attack.

Yiu-Chun Hu *et al*. [65] proposed a specific protocol namely TESLA with Instant Key disclosure (TIK), which is an extension of the TESLA broadcast authentication protocol to prevent wormhole attack in wireless networks. TIK is symmetric cryptographic primitive based on MAC. This scheme needs accurate time synchronization between all communicating parties and each communicating node to know just one public value for each sender node. Thus, TIK protocol enables scalable key distribution and also implements temporal leashes to enable the receiver to detect wormhole attack. The TESLA with instant key disclosure does not require

significant additional processing overhead at the MAC layer, however, it requires precise time synchronization, which is impractical to achieve in sensor network.

Jeffery et *al*. [66] presented a light-weight security protocol operated in the base station to enable to detect and remove the compromised node in sensor networks. This protocol does not specify any security measures in case of a passive attack on a node where an adversary is intercepting the communication. Moreover, this scheme increases the overhead of the neighbouring nodes of the base station. Later, Taejoon Park and K.G. Shin presented another Lightweight Security Protocol (LiSP) [67] equipped with efficient rekeying mechanism to tradeoff between security and resource consumption for large scale sensor network. LiSP uses a stream cipher for its cheap and fast processing. Also, LiSP supports periodic renewal of keys with inexpensive hash functions. However, the proposed scheme reduces resource consumption significantly and provides countermeasures against passive and active attacks, LiSP requires large storage capacity. Further, Riaz Ahamed *et al.* [68] introduced Lightweight Security (LSec) protocol for distributed sensor network. LSec provides authentication and authorisation phase with simple secure key exchange scheme. Confidentiality of data and protection mechanisms against intrusions and anomalies are ensured in LSec. LSec exhibits high scalability and memory efficiency. However, LSec suffered from higher communication overhead due to neighbouring nodes of base station by forwarding request and response packets during authentication and authorisation phase.

Lazos and Poovendran [69] propounded secure range-independent location to determine the location of sensors by using directional antennas, even in the presence of attackers. However, it is not feasible to use directional antennas, if sensor nodes are disguised by malevolent nodes. Later, Capkun and Hubaux [70] developed Secure Positioning In sensor NEtwork (SPINE) with nodes being deployed in an organized manner by using explicit RF distance bounding to obtain a verifiable location with the help of landmarks in the existence of adversaries. However, this algorithm is not suitable for random deployment in a scenario like battlefield application. Further, Anjum *et al*. presented a secure localization

algorithm [71] based on the transmission of nonce's power levels from anchor nodes. However, the performance of the proposed scheme will be poor, if the nodes exhaust its power.

Jing Deng *et al*. [44] introduced INSENS for wireless sensor networks. INSENS does not rely on detecting intrusions, but rather, tolerates intrusions by bypassing the malicious node. INSENS assumes that every node has a single symmetric key shared with base station. Since the base station uses a one-way hash chain to prevent malicious flooding, every node is additionally assumed to store the last element of the chain created by base station. The applicability of INSENS is strongly constrained by its centralized nature. Moreover, INSENS increases the traffic of the nodes in the close vicinity of the base stations by the centralized nature of the protocol.

SIGF is the first family of secured routing protocol for implicit geographic routing in sensor networks [45]. SIGF consists of three protocols that are built on each other. SIGF-0 is the first building block towards secure routing which selects the next-hop non-deterministically and dynamically. SIGF-1 is the extended version of SIGF-0 by maintaining and storing reputation information about the neighbours locally. Finally, SIGF-2 provides cryptographic defenses against malicious message manipulations and eavesdropping, including replay attacks. Therefore, SIGF-2 requires the most communication and computational effort but it gives the highest security warranty compared to the others. SIGF mitigates active attacks of network layer such as gray hole, black hole and sybil attack. The main problem with SIGF is the lack of source authentication. Since, SIGF provides hop-by-hop authentication, it is not sufficient to prevent the adversary from diverting the traffic to shorten the network lifetime. In addition, SIGF requires significant storage, communication and computation cost to provide source authentication.

Secure diffusion [46] is the secured protocol by using location-binding symmetric keys in the direct diffusion protocol [47]. The secured routing protocol adopts ideas of TESLA protocol to ensure authenticity and integrity of routing and

data information. Location binding keys are used by sink to authenticate the received sensing data and sensor nodes use pair-wise neighbour keys to establish secure gradients between the nodes. The disadvantage of the proposed scheme is the requirement of higher management cost at the base station for immense number of nodes.

SeRINS are the routing protocol which combines several existing security mechanisms together with its neighbour report system to ensure secure routing. The goal of SeRINS [48] is to protect the network against insider, which launches selective forwarding or advertise bogus routing information. SeRINS consist of three different schemes such as an alternate path scheme, neighbour report scheme and neighbour authentication. SeRINS are durable in the presence of several compromised nodes. However, detection and identification of maliciously packet dropping by nodes is not possible in the proposed scheme.

Wang Xiao-Yun *et al.* [72] presented Secure Low-Energy Adaptive Clustering Hierarchy (SLEACH) protocol for cluster based routing protocol, namely, LEACH [73] of sensor network. An efficient one-way hash chain and inexpensive symmetric operations are used in SLEACH. The proposed SLEACH scheme consists of four phases such as advertisement phase, cluster set-up phase, schedule creation phase and data transmission phase for security analysis. In each phase, inexpensive cryptographic operations are included to create an efficient secured routing protocol. Although, SLEACH is robust against external attacker or compromised node in the network, the proposed scheme reduces the lifetime of the cluster head due to increasing energy consumption.

Secure Hierarchical Energy-Efficient Routing protocol (SHEER) provides secure communication at the network layer. SHEER [74] mechanism uses a probabilistic broadcast mechanism and a three-level hierarchical clustering architecture to increase the lifetime. A hierarchical key management and authentication scheme is implemented in SHEER. High scalability, improved energy performance and increased lifetime are obtained through SHEER. However, SHEER reduces connectivity for coverage area greater than $500 \times 500 m^2$.

The secured routing protocols using cryptographic and hash chain techniques [75-78] either in the base station or in the node to defend against the routing attacks such as HELLO flood attacks, sybil attack, wormhole attack require excessive overhead, memory, time synchronization and complexity in configuring the nodes with encryption keys. Hence, it is essential to develop trust based security model for WSN by using the extended version of trust based mechanism of wireless adhoc networks [79-81] to reduce the overhead, complex computation and memory.

## 2.3 SUMMARY

It is evident from critical review of literature that exhaustive research work has already been done by several researchers to defend against attacks and improve the performance of sensor networks. Security mechanisms such as cryptographic techniques and authentication broadcast are developed to achieve better performance in the presence of external attackers. Further, different key management schemes based on key establishment and key pre-distribution mechanisms are explored to shield the network from internal attacks. Further more, intrusion detection and secured routing protocols using encryption and hash function were extensively studied to get rid of the network from external and internal attacks, and to enhance the network performance.

However, no attempt has been made so far to apply trust based security model in the routing protocols in sensor network with the available resources to evade sinkhole attack (black hole attack) for different coverage areas with large number of nodes considering mobility model to improve the performance of sensor network. Also, trust based framework in reactive routing protocols (DSR and AODV), location based routing protocols (GPSR and EGPSR) are yet to be explored to enhance the performance of sensor network in the presence of attackers. Hence, an attempt has been made in the present work to improve the performance of sensor network with trust based security mechanism incorporated in reactive and location routing protocols.

# CHAPTER 3

# TRUST BASED DYNAMIC SOURCE ROUTING PROTOCOL

## 3.1 INTRODUCTION

WSNs are expected to have applications in many areas such as homeland security, environmental monitoring and healthcare systems. Sensor nodes in the network are characterized by severely constrained energy resources and communicational capabilities. The main task of sensor nodes is to sense and collect data from a target domain, process the data and route the information to the specific sites where the underlying application resides. To achieve these potential, WSNs require novel routing techniques. Reactive routing protocols are one such type of routing techniques, where routes are created only on-demand by source node in order to preserve the precious node battery power. These routing protocols are exposed to different types of active attacks such as HELLO flood, selective forwarding and sinkhole attacks, when nodes are randomly deployed in a physically insecure environment. These attacks can inject malicious packets by compromising the node in the network. Secured reactive routing protocols have recently been developed by using cryptographic algorithms against these attacks. However, these secured routing protocols entail a number of prerequisites during both network establishment and operation phases. In contrast, trust based routing protocols developed for wireless networks use trusted route rather than the shortest routes in the network. An attempt has been made to implement a trust based dynamic source routing protocol for WSN considering sensing capabilities of nodes with dynamic configuration and increased scalability. TDSR is described in this chapter. The performance metrics of TDSR protocol are examined through simulation results and compared with DSR.

## 3.2 DYNAMIC SOURCE ROUTING PROTOCOL

DSR protocol is one of the reactive routing protocols. All data packets in the DSR protocol are affixed with source route header information that contains the complete list of nodes used for routing process [82]. So, the packet has to traverse in the order given in the source route header to reach a particular destination. Each intermediate node, upon receiving a data packet, forwards the packet to the next hop as listed in the source route header. Since, the route information is discovered only if source node is needed to forward the packet, DSR protocol is also known as on-demand protocol. The major difference between DSR protocol and other on-demand routing protocols (AODV) is that DSR protocol is beaconless and hence does not require periodic hello packet (beacon) transmissions, which are used by node to inform its neighbours of its presence. DSR protocol consists of two phases such as route discovery and route maintenance [83].

During route discovery phase, the source node broadcasts a ROUTE REQUEST packet with a unique identification number which is flooded through the network in a controlled manner. The ROUTE REQUEST packet broadcasted by the source node contains the address of the destination node to which a route is desired [84]. The nodes which have no information regarding the destination node or have seen the ROUTE REQUEST packet for the first time append their Internet Protocol (IP) addresses to the ROUTE REQUEST packet and rebroadcast it. The ROUTE REQUEST keeps on spreading until they reach the target node or any other node that has a route to the target node. The Time To Live (TTL) field in IP address is being incremented in each route discovery to control the spread of ROUTE REQUEST packet by doing the broadcast in a non-propagating manner. Route discovery process with ROUTE REQUEST mechanism is shown in Figure 3.1.

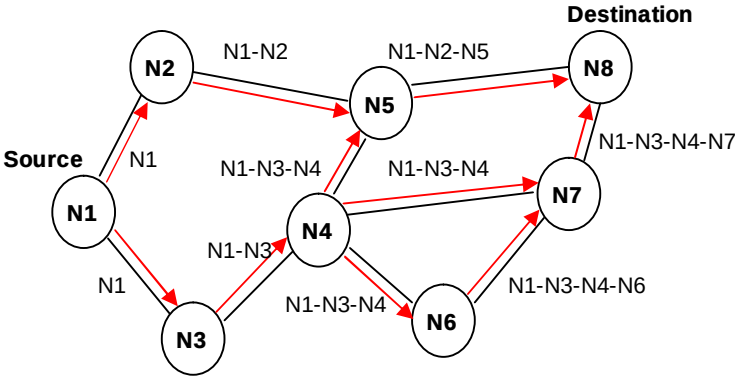


**Figure 3.1 Route discovery process with route request**

The destination node or the node which has a route to destination answers in the form of ROUTE REPLY packet for the first received ROUTE REQUEST packet. The ROUTE REPLY packet contains the complete list of nodes through which the ROUTE REQUEST packet had traversed. Route discovery process with ROUTE REPLY scheme is illustrated in Figure 3.2.

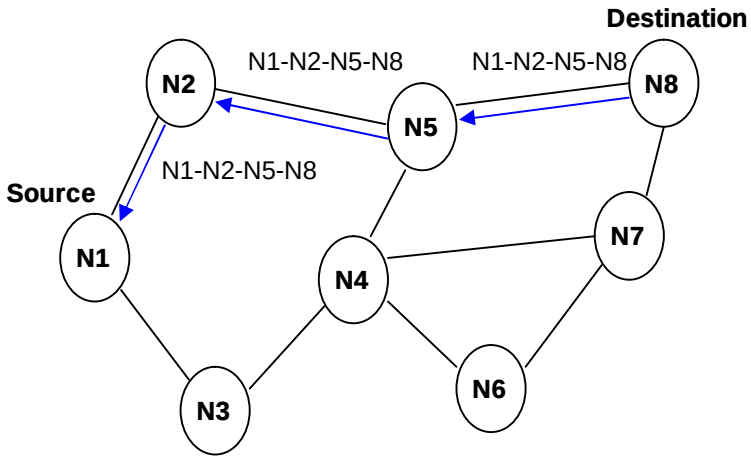


**Figure 3.2 Route discovery process with route reply**

The major limitation of this protocol is that the route maintenance mechanism does not locally repair a broken link. DSR protocol stores all usable routing information extracted from overhearing packets for updating the ROUTE CACHE mechanism of the node which leads the node to use a wrong path to send data or to reply with invalid route information to other ROUTE REQUEST.

The other drawback of DSR protocol is that this protocol is exposed to sinkhole attack by deploying the nodes in unsupervised environment. Sinkhole attacks [11] lure other sensor nodes to route most of the traffic towards the compromised nodes which is described in Figure 3.3. The impact of sinkhole attacks is that they can be used to launch another type of active attack named selective forwarding by compromising the node as malicious node, which attract the neighbour nodes to forward selectively certain packets through that malevolent node. Hence, the packet loss and routing overhead of DSR protocol are increased in the presence of active attacks. To reduce the packet loss, secured reactive routing protocols are developed using cryptographic and hash functions [75-78]. However, these secured cryptographic routing protocol schemes require excessive overhead which increases the computational complexity. To overcome these limitations, trust based framework has been introduced for wireless networks [80] by reducing the packet loss and routing overhead and eliminating the compromised nodes.

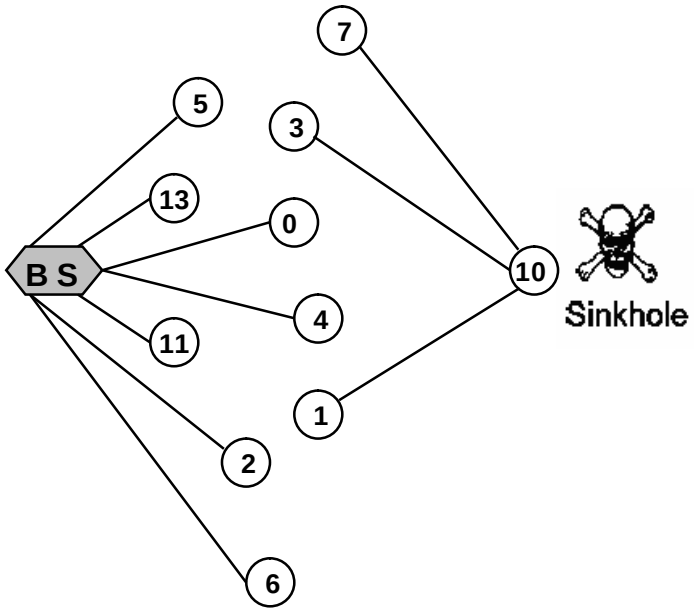


**Figure 3.3 Sinkhole attack**

The trust model essentially performs the function of trust derivation, computation and application [81]. During trust derivation, each node derives trust levels from directly experienced events. Next in trust computation, the monitored events are normalised and assigned weights so as to compute the direct trust in other nodes. These computed levels are then associated with the routing process during trust application.

## 3.3 TRUST BASED DYNAMIC SOURCE ROUTING PROTOCOL

The extended version of TDSR of ad hoc network is developed for WSN by appending the sensing agent module to the nodes. Each sensor node executing the trust based dynamic source routing protocol model, measures the accuracy and authenticity of its immediate neighbouring sensor nodes by monitoring their participation in the packet forwarding mechanism [85]. Detection and evasion process are used in TDSR to eliminate malevolent nodes. The flow chart of TDSR protocol for WSN is shown in Figure 3.4.

### 3.3.1 Detection Process

Each sensor node before transmission of a data packet, buffers the DSR source route header with (DSR_Agent::buffer_packet). After transmitting the packet, the node places its wireless interface into the promiscuous mode for Trust Update Interval (TUI). The TUI represents the time; a sending node must wait after transmitting a packet until it overhears the transmission of the forwarded packet by its neighbour [81]. This interval is critically related to the mobility and traffic of the network. If this interval is made too small, it may result in ignoring of the transmissions by an inefficient neighbour. Similarly, a large TUI value will cause energy costs and also induce errors due to nodes getting out of reception range. If the packet is forwarded by the neighbour node without any alteration within the TUI, its corresponding Trust Level Counter (TLC) is incremented indicating the absence of sinkhole attack. If the packet is not forwarded or altered in an unexpected manner within the TUI, its corresponding TLC is decremented. This state indicates the presence of sinkhole attack. In case, a timeout occurs when TUI is expired, DSR source route buffer is cleared for the timeout condition.

The sending node also verifies the different fields of source route header in the forwarded IP packet for requisite modifications through a sequence of integrity checks. If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its direct trust is incremented. This condition indicates the absence of malicious node. On the other hand, if the integrity check fails or the forwarding node does not transmit the packet at all, then its corresponding Direct Trust Measure (DTM) is decremented. Hence, that particular node is treated as malevolent node.

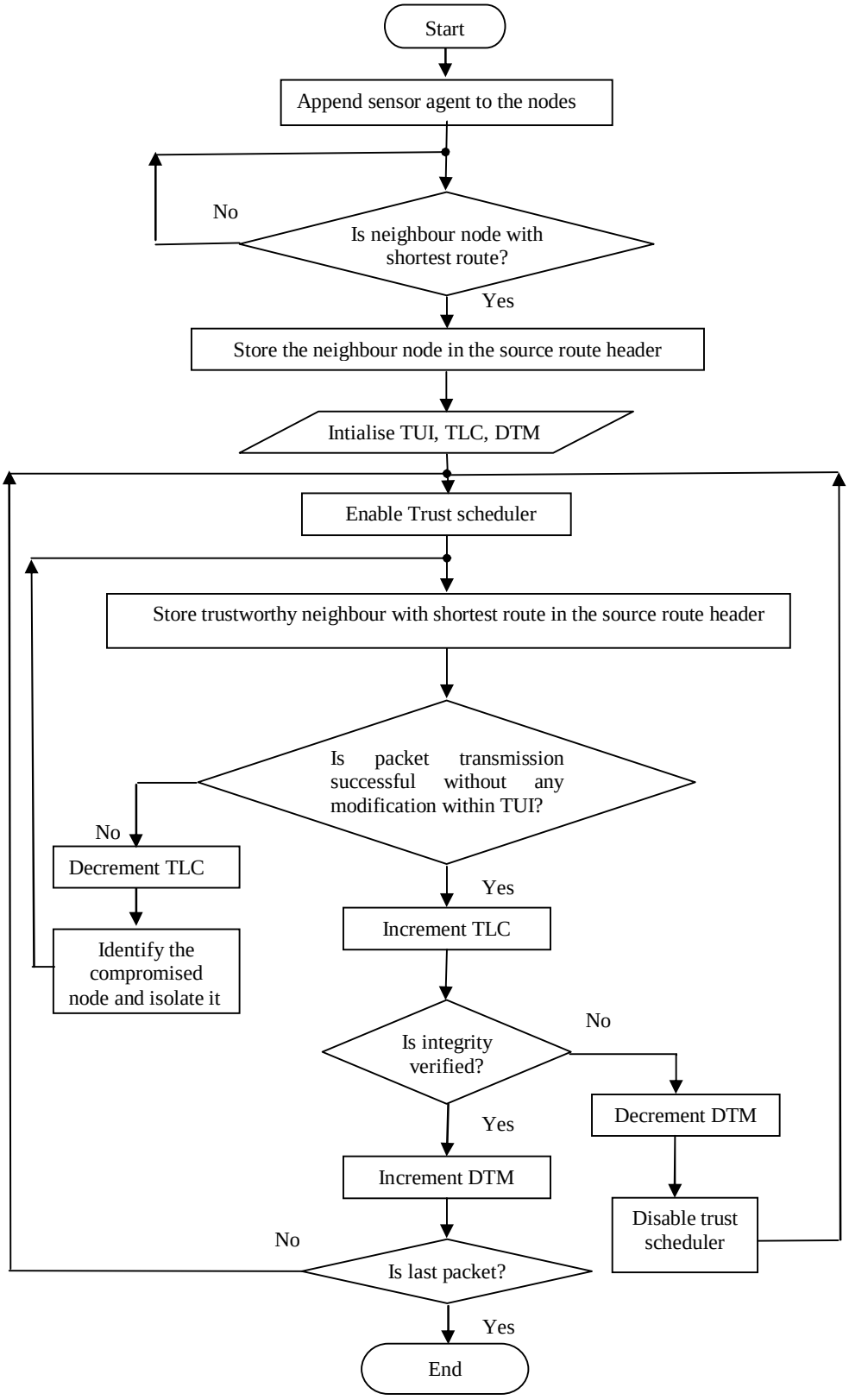


**Figure 3.4 Flow chart of TDSR protocol**

### 3.3.2 Evasion Process

With the standard DSR protocol, all immediate nodes blindly forward the packets to the succeeding nodes having the shortest path as listed in the source route header whereas in TDSR, the trusted path is used to evade any possible sinkholes. TDSR verifies the trust levels of all remaining nodes present in the packet's source route header [86], instead of checking the connectivity of the next hop in case of mobile nodes. If the malicious mobile nodes are not present, the packets are forwarded as per the source route header. Otherwise, alternate route is identified to forward the packet.

## 3.4 SIMULATION RESULTS AND DISCUSSION

The trust model is implemented in the existing DSR protocol to obtain the TDSR protocol considering two trust levels T1 (trust update interval of 5seconds) and T2 (trust update interval of 7seconds). The TDSR protocol is simulated using network simulator (ns-2.30) [97] to emulate sinkhole attacks in the mobile sensor network. The performance parameters such as delivery ratio, routing overhead and delay are determined by varying the number of malicious nodes from 5 to 40. The parameters used in the simulation are listed in Table 3.1.

**Table 3.1 Simulation parameters for TDSR**

| **Simulation Parameters** | **Values** |
|---|---|
| Number of nodes | 150 and 200 |
| Geographical area ($m^2$) | 300×300 and 500×500 |
| Number of malicious nodes | 5 to 40 |
| Packet size(bytes) | 512 |
| Mobility model | Random way point |
| Pause time(s) | 20 |
| Trust update interval(s) | 5 and 7 |
| Simulation time (s) | 100 |

The sample Network AniMator (NAM) output is shown in Figure 3.5 for the mobile sensor network of 150 nodes with ten malicious nodes indicated by red colour circles. Using TDSR protocol, the packets will be forwarded successfully from the source node to the destination node by using trusted path which eliminates the compromised nodes.

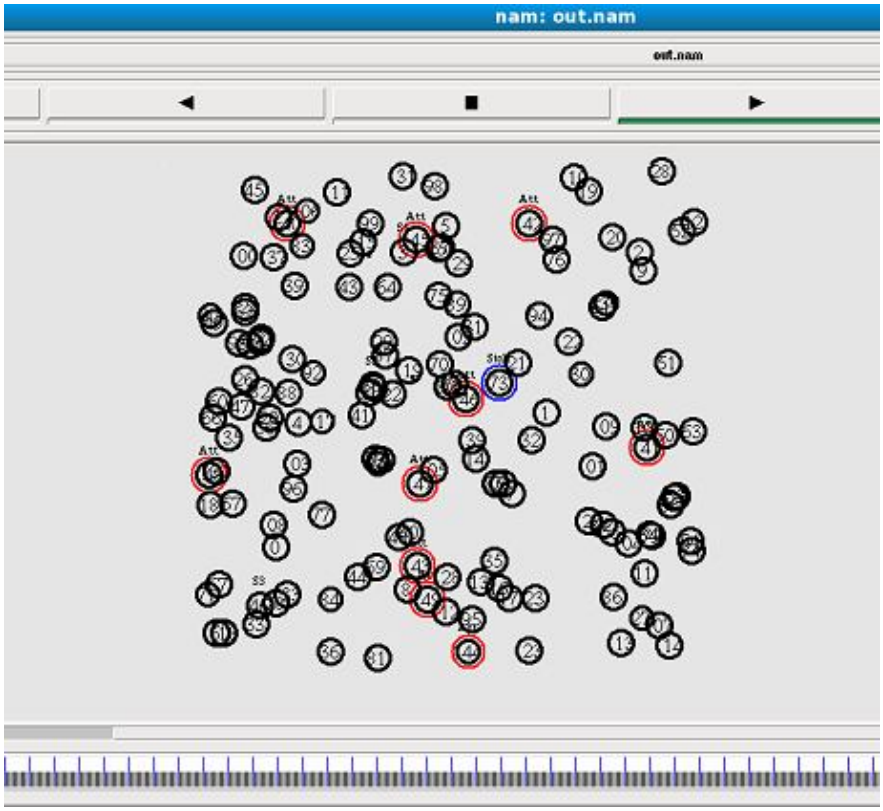


**Figure 3.5 NAM output of TDSR for 150 nodes with ten malicious nodes**

### 3.4.1 Delivery Ratio

Delivery ratio of TDSR (T1 and T2) with the number of malicious nodes varying from 5 to 40 i) for 150 with coverage area of 300×300m$^2$ (Figure3.6) ii) for 150 with coverage area of 500×500m$^2$ (Figure3.7) iii) for 200 nodes with coverage area of 300×300m$^2$ (Figure3.8) and iv) for 200 nodes with coverage area of 500×500m$^2$ (Figure3.9). It is observed from the results that delivery ratio of TDSR is higher than that of DSR. From the Figure 3.7, it is found that TDSR outperforms DSR by providing significant improvement in delivery ratio of around 23% and 45% for trust levels T1 and T2 respectively considering 10 malicious nodes. The

improvement in the delivery ratio is due to the increment in the forwarding rate of packets using trusted path rather than the shortest path from source to destination by eliminating the attackers. Figure 3.8 and Figure 3.9 depict that TDSR with 200 nodes has greater delivery ratio than that of TDSR with 150 nodes. The increased delivery ratio in case of 200 nodes is due to the availability of more trusted route than that of 150 nodes.

From the Figure 3.7 and Figure 3.9 it is demonstrated that the delivery ratio of TDSR is reduced for increased coverage area of 500×500m$^2$ compared to that of coverage area of 300×300m$^2$. The reduction in the delivery ratio for 500×500m$^2$ is due to the more random deployment of nodes which reduces the forwarding rate in that coverage area.

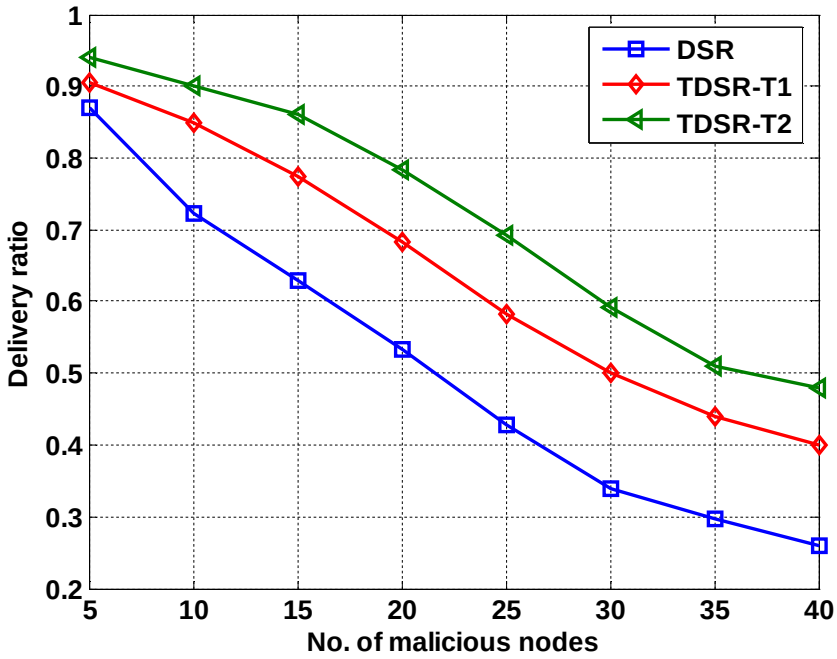


**Figure 3.6 Delivery ratio of TDSR with different number of malicious nodes for 150 nodes with coverage area 300×300 m$^2$**

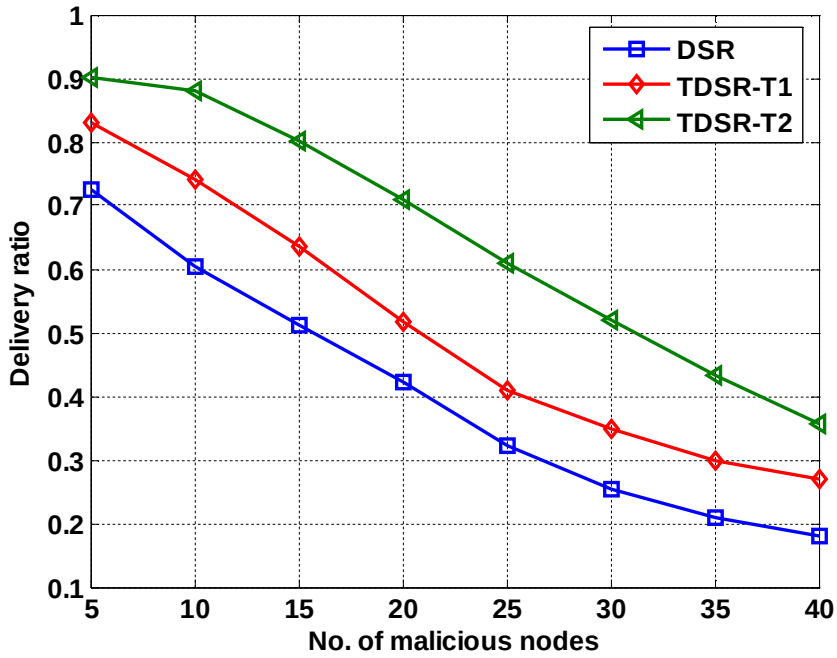


**Figure 3.7** **Delivery ratio of TDSR with different number of malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

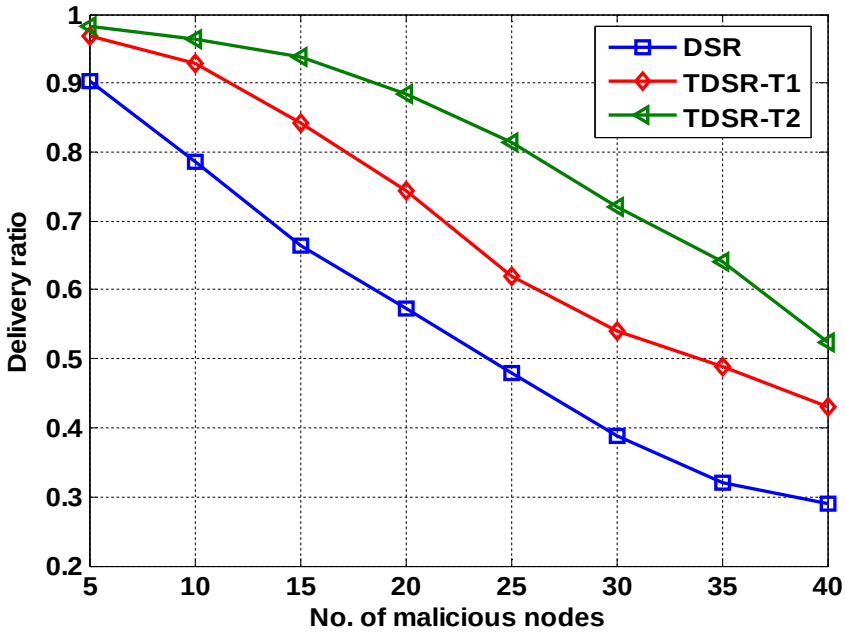


**Figure 3.8** **Delivery ratio of TDSR with different number of malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

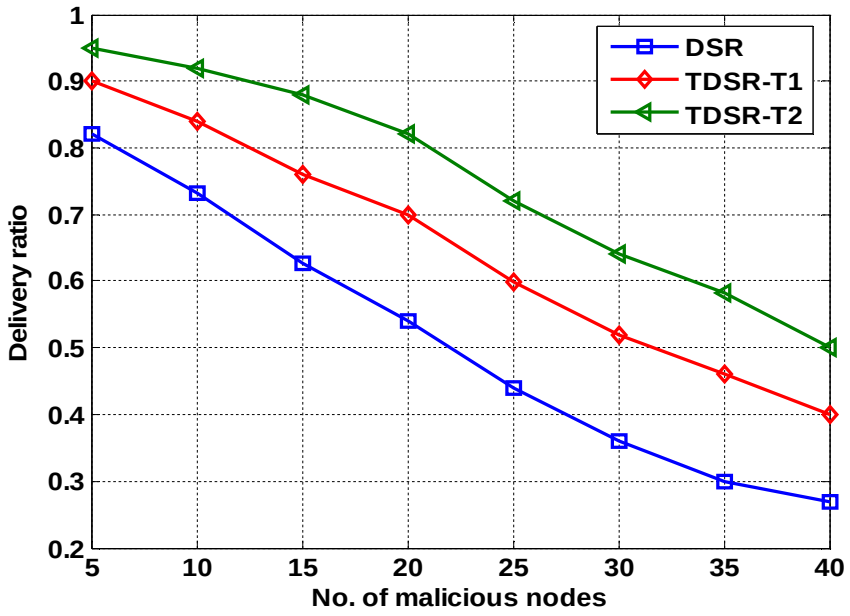


**Figure 3.9 Delivery ratio of TDSR with different number of malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

### 3.4.2 Routing Overhead

TDSR has an overall lower routing overhead compared to that of DSR which is illustrated by the Figure 3.10 to Figure 3.13. Even though, routing overhead increases with the increase of malicious nodes, TDSR achieves significant reduction in routing overhead of about 64% and 67% compared to that of DSR for trust levels T1 and T2 respectively considering malicious node of 40 which is shown in Figure 3.10. The reduced overhead is due to less number of control packets generated for each data packet and increased forwarding rate in TDSR. However, routing overhead is higher for coverage area of 500×500$m^2$ (Figure 3.11 and Figure 3.13) than that of coverage area 300×300$m^2$ (Figure 3.10 and Figure 3.12). The increased routing overhead for 500×500$m^2$ is due to the increased control packets and reduced forwarding rate.

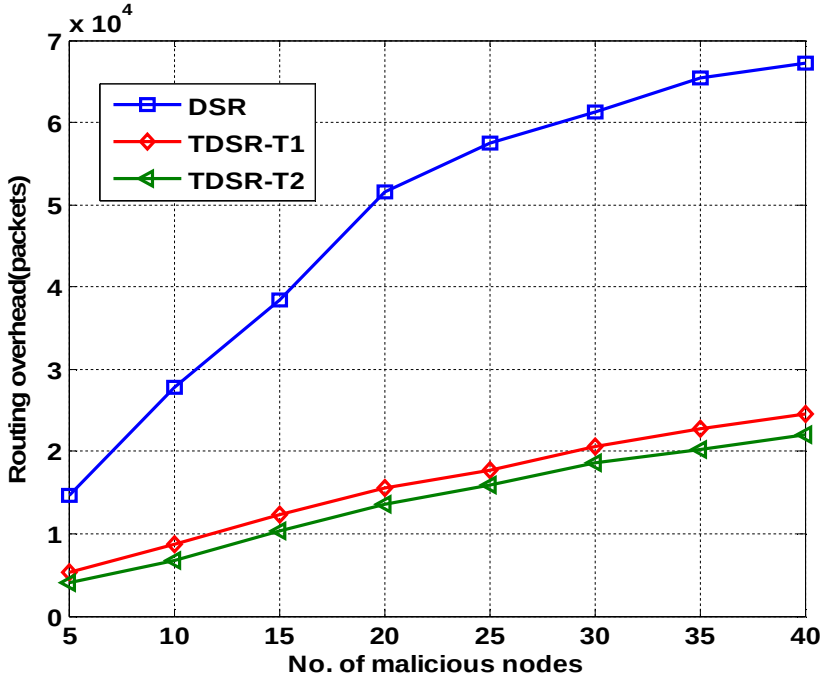


**Figure 3.10** **Routing overhead of TDSR with respect to malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

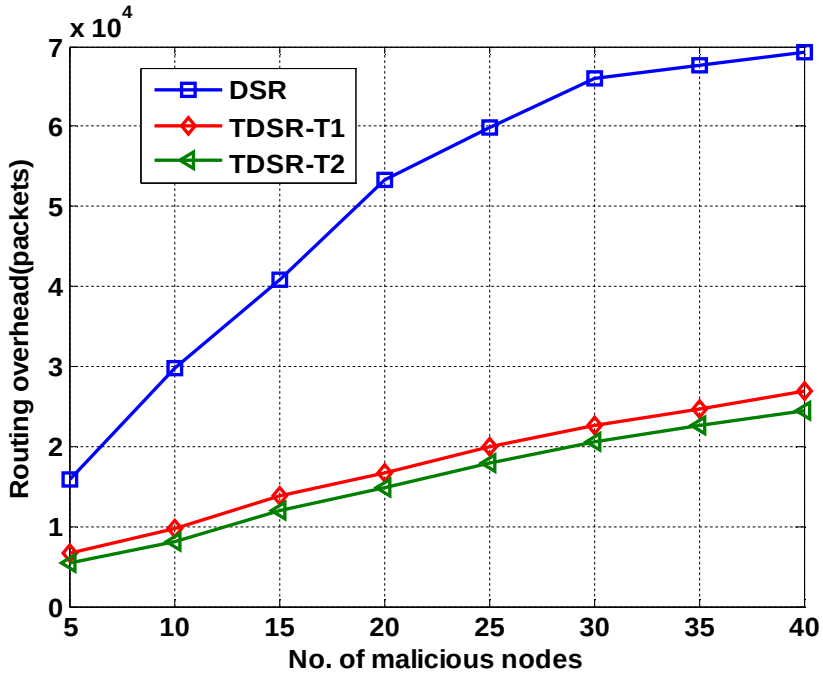


**Figure 3.11** **Routing overhead of TDSR with respect to malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

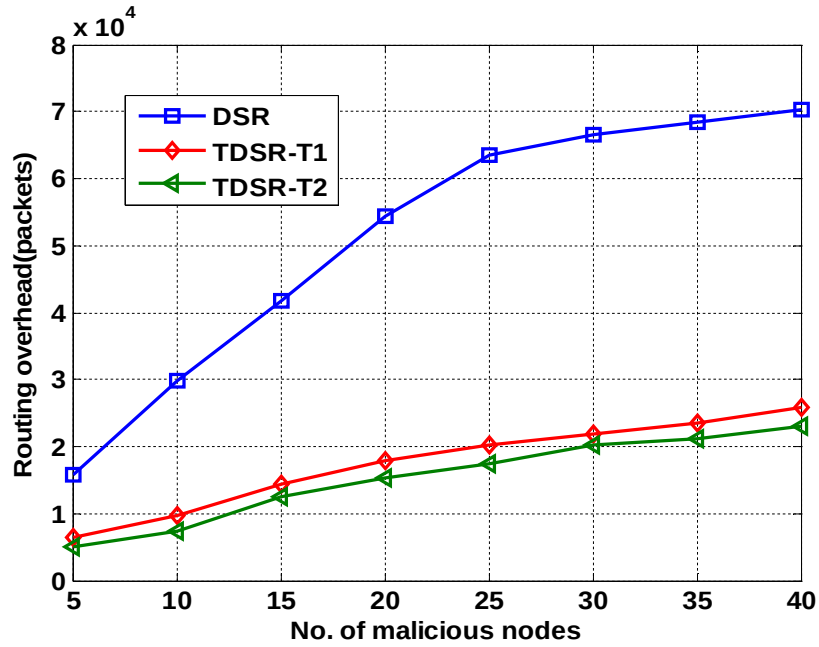


**Figure 3.12** **Routing overhead of TDSR with respect to malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

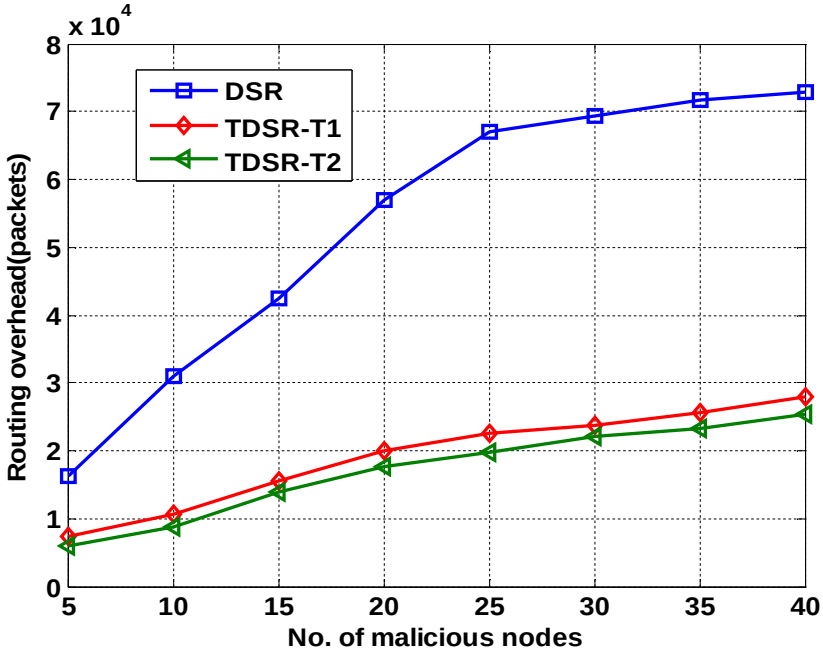


**Figure 3.13** **Routing overhead of TDSR with respect to malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

### 3.4.3 End to End Delay

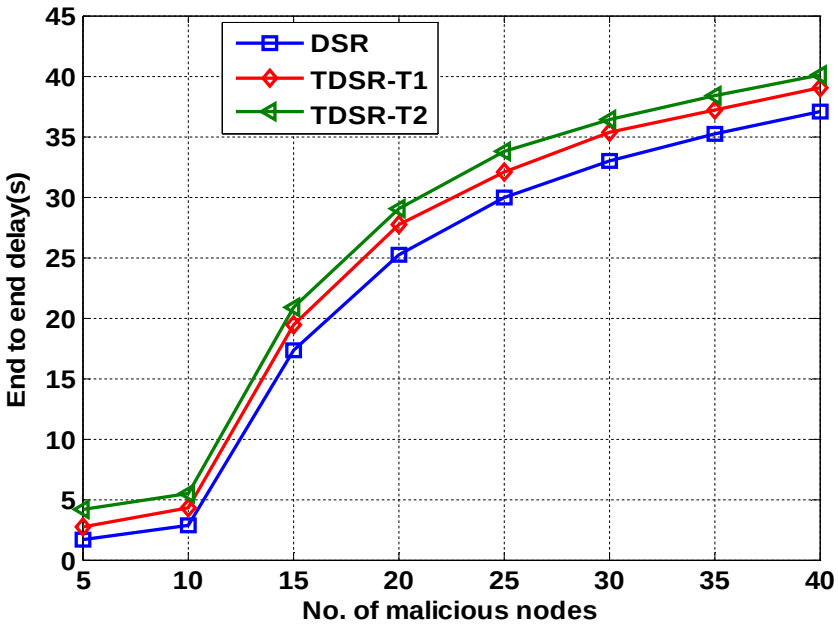


**Figure 3.14** **End to end delay of TDSR for various malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

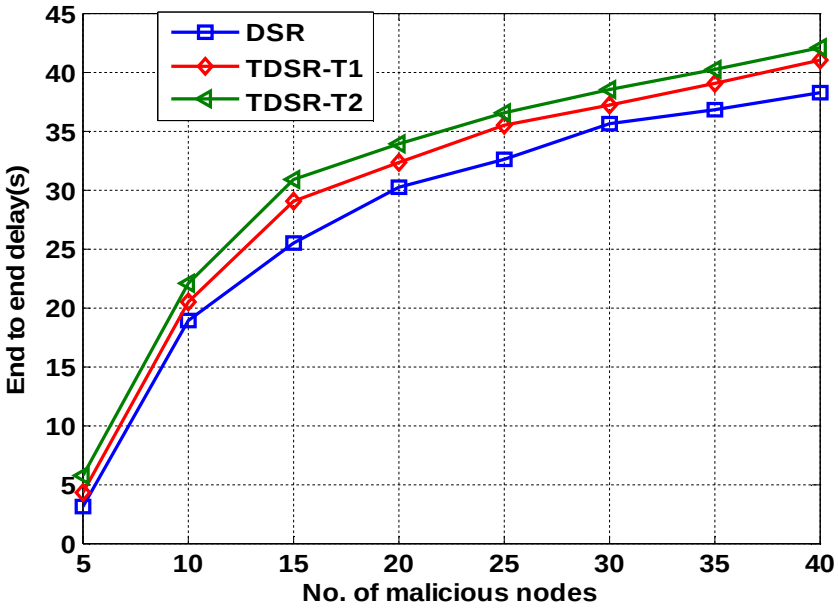


**Figure 3.15** **End to end delay of TDSR for various malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

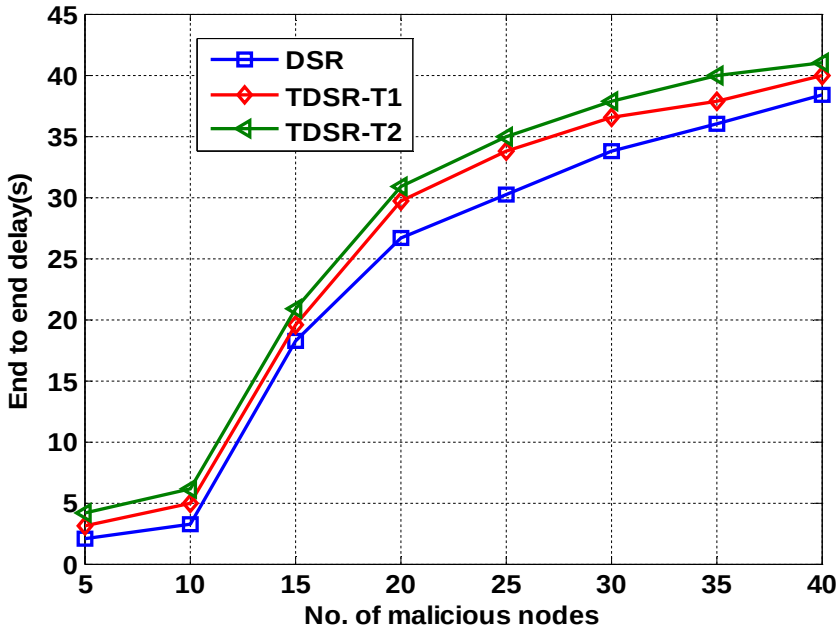


**Figure 3.16** **End to end delay of TDSR for various malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

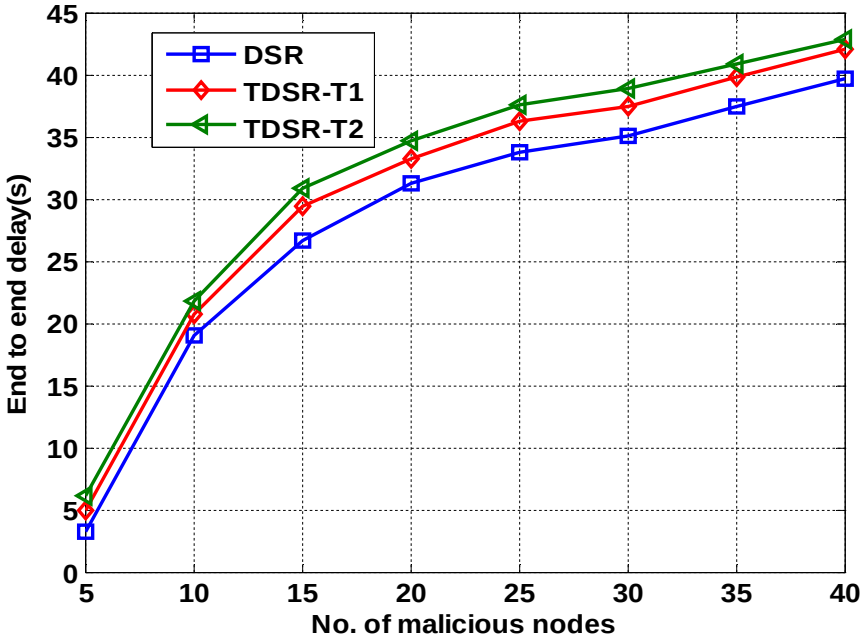


**Figure 3.17** **End to end delay of TDSR for various malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

Simulation results shown from Figure 3.14 to Figure 3.17 portray that delay of TDSR protocol is higher than that of DSR protocol for 150 and 200 nodes with different coverage area 300×300 $m^2$ and 500×500 $m^2$. Figure 3.14 depicts that delay of TDSR protocol is increased between 5% to 6% and 8% to 9% for T1 and T2 respectively for various malicious nodes, which is higher than that of DSR protocol. The increment in the delay is due to the fact that, the routes used in TDSR are trusted routes rather than the shortest routes to transmit the packets from source node to target node by avoiding the compromised nodes. The increased delay is the penalty factor which has to be endured for reduced packet loss achieved through TDSR.

## 3.5 CONCLUSION

TDSR protocol is implemented for mobile sensor network by using ns-2.30. The performance parameters such as delivery ratio, routing overhead and delay of TDSR are determined and also compared with DSR protocol by varying the number of malicious nodes from 5 to 40 considering 150 and 200 nodes for different coverage areas of 300×300 $m^2$ and 500×500 $m^2$ with two trust levels T1 and T2 respectively. The results show that an improvement of 43% in delivery ratio and reduction of 66% in routing overhead for higher values of malicious nodes is achieved using the TDSR protocol than the standard DSR protocol for T2 level. This is mainly due to the trusted path chosen by TDSR having trusted nodes to get rid of the nodes that were acting as sinkhole attacks. However, the delay of TDSR protocol is higher than that of DSR.

# CHAPTER 4

# TRUST BASED ADHOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

## 4.1 INTRODUCTION

AODV is another on-demand routing protocol in which the routes are created only when source has packets to transmit to the destination. Routes of AODV are maintained as long as they are required by the source for data transmission. The AODV protocol usually uses distance vector routing algorithms that maintain only the information about next hop to immediate neighbours resulting in improved network performance. However, the performance of AODV is degraded in the presence of malicious nodes. To achieve enhanced performance, the trust based adhoc on demand distance vector routing protocol (TAODV) is developed for wireless networks by isolating the compromised nodes. TAODV for WSN is anticipated by appending sensing capabilities to the nodes with increased scalability. TAODV is described in this chapter and the performance parameters of TAODV protocol such as delivery ratio, routing overhead and end to end delay are studied through simulation results and compared with AODV.

## 4.2 ADHOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

AODV is a reactive routing protocol which achieves better performance for the nodes having dynamic configuration. It uses traditional routing tables, one route entry per destination and Destination Sequence Number (DSN) to ensure the

freshness of routes and avoid the routing loops [84]. This will greatly increase the efficiency of routing processes. The protocol forwards the packet by using two routing phases along with the help of control messages which are described below.

### 4.2.1 Control Messages in AODV

Control messages are used for the discovery and breakage of routes in AODV. The various types of control messages used in the routing process of AODV are Route REQuest message (RREQ), Route REPly message (RREP), Route ERRor message (RERR) and HELLO messages.

***Route Request***

A RREQ packet is flooded throughout the network when a route is not available from the source node to the destination. The following fields are contained in the RREQ packet which is shown in Figure 4.1.

| Source address | Request ID | Source sequence number | Destination address | Destination sequence number | Hop count |
|---|---|---|---|---|---|

**Figure 4.1 Route request format**

The RREQ is identified by the pair source address and request ID. Each time, when the source node sends a new RREQ, the request ID is then incremented [87]. On receiving a RREQ message, each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters, the new RREQ packet will be discarded. Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP message by considering the following criteria. The first criterion is that if the node has no route

entry for the destination, or the available route entry is not an up-to-date route, the RREQ will be rebroadcasted with incremented hop count. The second one is that if the node has a route with a sequence number greater than or equal to that of RREQ, a RREP message will be generated and sent back to the source.

***Route Reply***

If a node has a valid route to the destination or is the destination itself, it unicasts a RREP message back to the source. This message contains the following fields illustrated in Figure 4.2.

| Source address | Destination Address | Destination sequence number | Hop count | Life time |
|---|---|---|---|---|

**Figure 4.2 Route reply format**

***Route Error Message***

All the nodes monitor their own neighbourhood nodes. When a node in an active route is lost, a RERR is generated to notify the other nodes on both sides of the link of this lost link.

***Hello Messages***

The HELLO messages are broadcasted by each node in order to know its neighbourhood nodes so that the neighbour nodes are directly communicated with it. Further, these messages also inform the neighbours about the existence of the link [88] and will be forwarded until the value of TTL=1.

### 4.2.2 Route Discovery and Route Maintenance

AODV has two basic operations such as route discovery and route maintenance used for transmitting the packet from the source to the required destination [89].

***Route Discovery***

Route discovery is initiated when a source node wants to find a route to a new destination or when the lifetime of an existing route to the destination has expired. The process is initiated by broadcasting the RREQ as shown in Figure 4.3. The source node broadcasts a RREQ packet to its neighbours until the sought route is discovered. Upon receiving a RREQ, neighbour node checks whether the sought route is a 'fresh enough' route using its DSN. If the DSN of the sought route is greater than DSN of RREQ, the route is said to be a 'fresh enough' route. Then the neighbouring node replies with a RREP packet to the source node. The RREP is traveled through the reverse path noted by each node during the transmission of RREQ. Then the source node establishes the forward path for the data transmission during the transmission of the RREP message.

***Route Maintenance***

To maintain connectivity, nodes either periodically broadcast HELLO packets to their neighbours or use acknowledgement based mechanisms at the link or network layers [90]. Upon detecting a link break, a node could choose to repair the link locally (if the destination is no farther than MAX_REPAIR_TTL hops away) or send a RERR packet to notify its upstream nodes. A RERR message contains the list of those destinations which are not reachable due to the loss of connectivity.

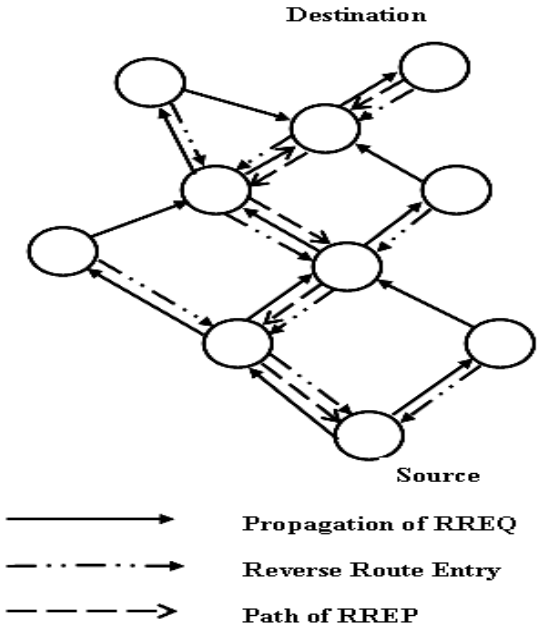


**Figure 4.3 Discovery of route**

Although, AODV has improved performance in terms of forwarding rate and delay for increased mobile nodes, the performance will be degraded in the presence of malevolent nodes. To enhance the performance of wireless networks, trust based AODV protocol TAODV is propounded by eliminating the malicious nodes.

## 4.3 TRUST BASED ADHOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The improved version of TAODV is anticipated for WSN by adding sensing module to the nodes. The salient features of TAODV [90] are

- Each node maintains an additional data structure called the neighbours' trust table. The trust table contains neighbouring node IDs, their corresponding trust values and the current number of route requests which are sent by the node.

- Each route table entry for a given destination stores all the routes from the source node to the destination with the highest DSN. The corresponding route trust values as advertised by the intermediate nodes termed as Advertised route Trust Value (ATV) and the computed Route Selection Value (RSV) are stored in the route table. Each route to a destination is identified by unique Route ID say '$R_{id}$'. The $R_{id}$ with the highest RSV is stored in the advertised $R_{id}$ field and advertised to the upstream nodes.

- The RREQ packet of TAODV has two additional fields: the omit node flag and the omit node ID. The omit node flag, if set, indicates that the node ID mentioned in the omit node ID field should be precluded from the route to the destination. The rest of the RREQ packet is same as that in the AODV protocol.

- The RREP packet has additional fields to accommodate the route trust and the recommender node's ID. For every RREP, the intermediate node increments the number of hops by one and caches the route trust sent by the downstream node from its route trust field. Otherwise, if the node has individually computed its own trust value on the route, then it updates the route trust and the recommender node ID fields with its own route trust value and node ID.

- R_ACK is the modified version of the RREP ACKnowledgment (RREP-ACK) message of the AODV protocol. The RREP-ACK is used to acknowledge the receipt of a RREP over an unreliable link. Apart from performing the same task as RREP-ACK, a R_ACK functions as a report packet. A report packet would be initiated by the destination to inform the source and the intermediate nodes about the number of packets it received so far since the last transmission of R_ACK.

### 4.3.1 Trust Framework and Computation

There are two trust values associated with the TAODV protocol. They are route trust and node trust. Route trust is a measure of the reliability with which a packet can reach the destination, if forwarded by the node on that particular route. Node trust is computed based on the difference between the nodes' ATV to the destination and the Observed Trust Value (OTV) computed for the current data transfer.

***Route Trust***

Route trust is computed by every node for each route in its routing table. The route trusts are initially unknown. RREQ's are sent by source node S and the routes are established to the destination node D as in AODV. All RREQs of the intermediate nodes having fresh enough routes are able to establish reverse route from D to S. Each node keeps track of the number of packets it has forwarded through a route. D periodically sends R_ACK packets to S at an agreed interval between S and D. Each intermediate node on the reverse route from D to S checks the R_ACK packets to compute its route trust. Route trust is calculated as a ratio of the number of packets received at D to the number of packets forwarded by the node under consideration (from S to D on that route).

***Node Trust***

Every node also maintains node trust on each of its neighbours. Initially when the network is setup, the proposed scheme functions almost like AODV. In the beginning, a node does not have any trust level information of the neighbour nodes, i.e., they can neither be fully trusted nor be fully distrusted. So all nodes have 50% initial node trust and this trust remains unchanged before forwarding the packet. When a node 'i' forwards or generates a RREP, i advertise its trust on the route under consideration to its immediate upstream node P. Node P caches this route trust value as ATV of node i on that route and compares it with the OTV. The node 'i'

receives an incentive if the OTV is within an admissible range of ATV. Then the node P allows the node i to forward the packets [91]. This indicates the absence of compromised nodes (sinkhole attack). Otherwise, the node i is penalized, i.e., node P isolates the node i by not forwarding the packets and not entertaining any RREQs which indicates that the node is identified as malicious node. Then the node P finds alternate node to transmit the packet to the destination. The penalties and the incentives are inversely proportional to the node's distance from the destination. For example, the node farther away from the destination has lesser information on the downstream nodes' behaviour. A node which is only one-hop from the destination is solely responsible for packets reaching the destination. So its trust on the route is based only on its own behaviour and link between itself and the destination.

### 4.3.2 Route Selection Criteria

The node S may get several RREP packets in response to its RREQ packet to D. The route selection criterion is dependent on node trust of the immediate downstream neighbour node N that recommended the route, and on route trust node N has on the sought route. The route selection criterion is inversely proportional to the number of hops in the route. In this scheme, a source node calculates the RSV for all its available routes to the destination and it finally chooses the route which has the highest RSV. If two routes have the same RSV then the following norms are used to break the tie. The first condition is that the routes with highest route trust are selected. The second criterion is that if the routes have same route trust values then the route with the highest immediate downstream neighbours' node trust (as perceived by the source/immediate upstream node) is chosen. The third one is that if the immediate downstream neighbours' node trust is also the same, then the shortest route is chosen. If all the above are same then it will choose randomly among those routes with same RSVs which is mentioned as final condition. The flow chart of TAODV is shown in Figure 4.4.

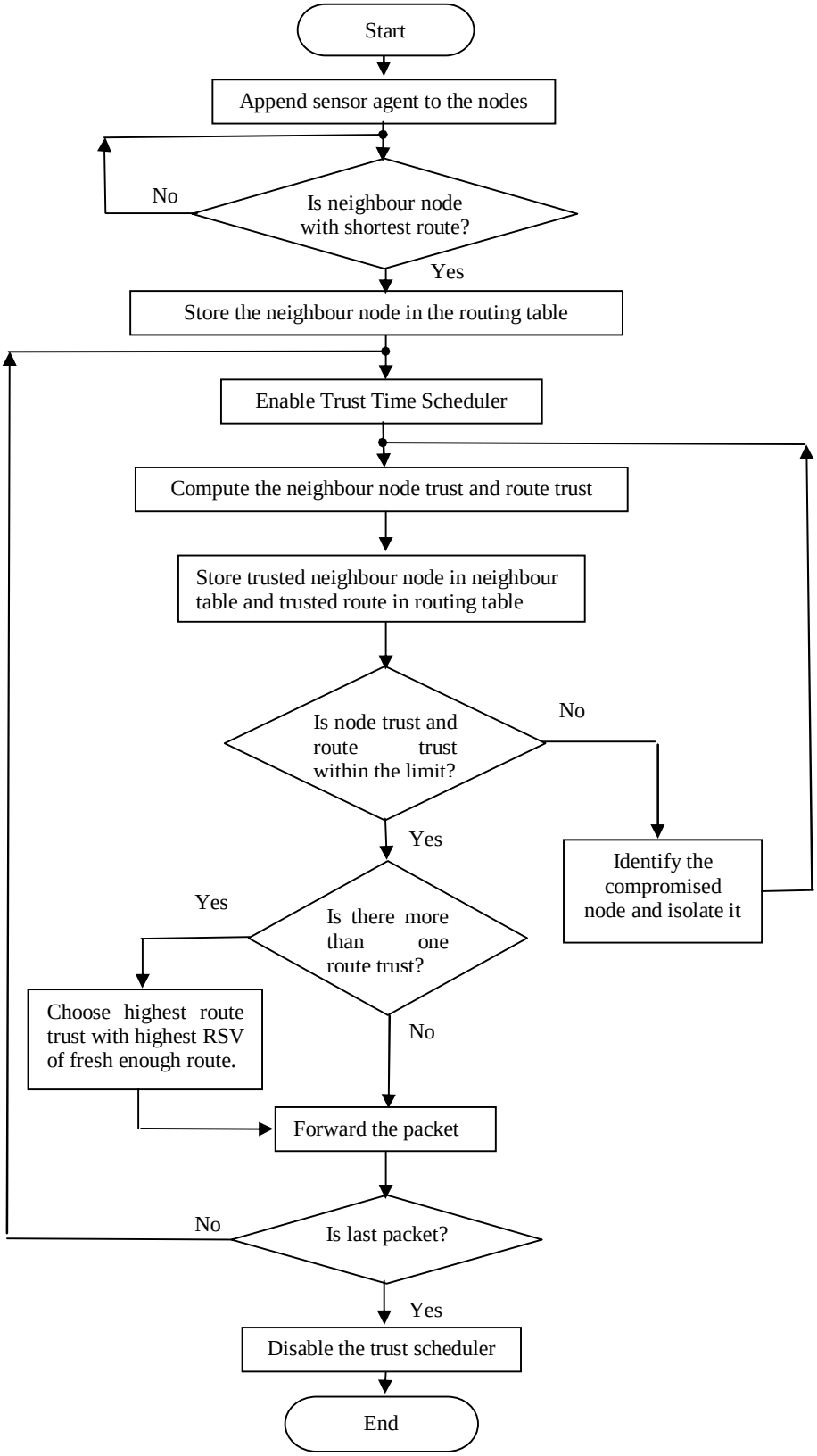


**Figure 4.4 Flow chart of TAODV protocol**

## 4.4 SIMULATION RESULTS AND DISCUSSION

The trust and mobility model is implemented in the existing AODV protocol to obtain the TAODV protocol for trust levels T1 and T2 respectively. The TAODV protocol is simulated using ns-2.32 [97] to emulate compromised nodes. The performance parameters such as delivery ratio, routing overhead and delay are determined for 150 and 200 nodes by varying the number of malicious nodes from 5 to 40 with various coverage areas such as 300×300$m^2$ and 500×500 $m^2$. The parameters used in the simulation are listed in Table 4.1.

**Table 4.1. Simulation parameters for TAODV**

| **Simulation Parameters** | **Values** |
|---|---|
| Number of Nodes | 150 and 200 |
| Geographical area($m^2$) | 300×300 and 500×500 |
| Number of malicious nodes | 5 to 40 |
| Packet Size(bytes) | 512 |
| Trust update interval(s) | 5 and 7 |
| Mobility model | Random way point |
| Pause time(s) | 20 |
| Simulation time(s) | 100 |

### 4.4.1 Delivery Ratio

Delivery ratio of TAODV is higher than that of AODV i) for 150 nodes with coverage area of 300×300$m^2$ (Figure 4.5) ii) for 150 nodes with coverage area of 500×500 $m^2$ (Figure 4.6) iii) for 200 nodes with coverage area of 300×300$m^2$ (Figure 4.7) and iv) for 200 nodes with 500×500$m^2$ (Figure 4.8). TAODV outperforms AODV by providing delivery ratio of nearly 30% and 60 % considering

T1 and T2 respectively for 150 nodes which is illustrated in Figure 4.5. Also, Figure 4.6 reveals that there is an increment in the delivery ratio of TAODV by approximately 23 % and 53 % compared to that of AODV for T1 and T2 respectively with coverage area 500×500$m^2$.

TAODV achieves improved delivery ratio due to increased forwarding rate of packets transmitted from source to destination by utilising trusted path along with the shortest route. Moreover, TAODV selects or deselects the neighbour node for routing process based on their node trust and route trust to avoid the malicious node.

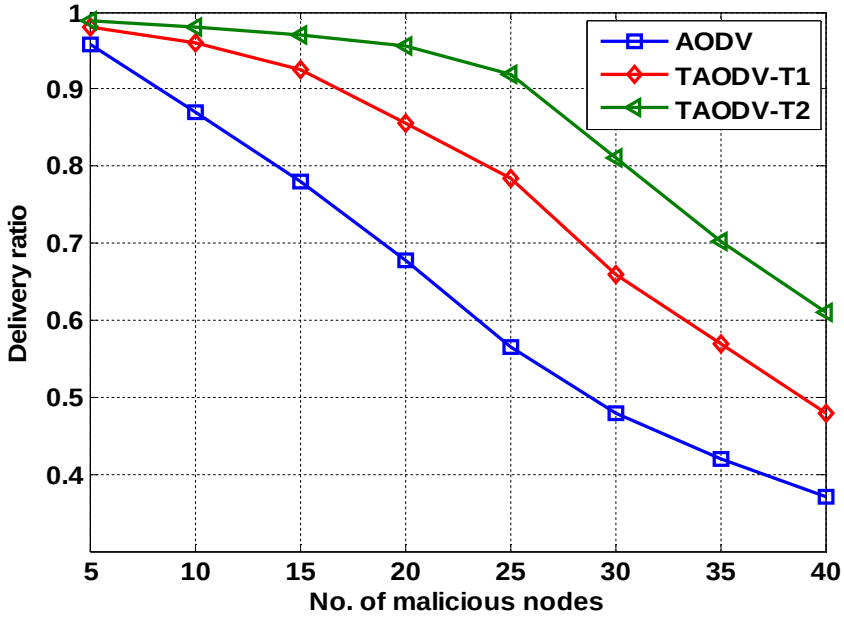


**Figure 4.5 Delivery ratio of TAODV for different number of malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

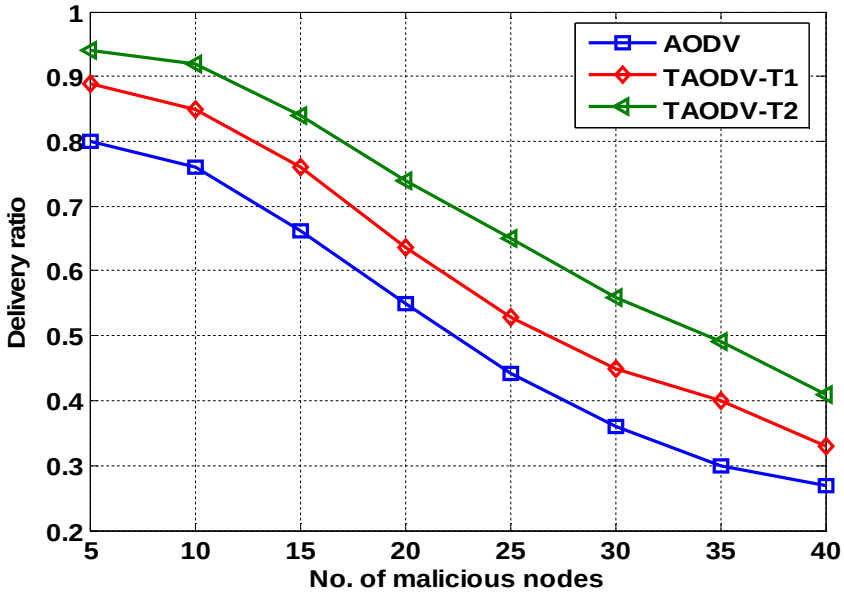


**Figure 4.6** **Delivery ratio of TAODV for different number of malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

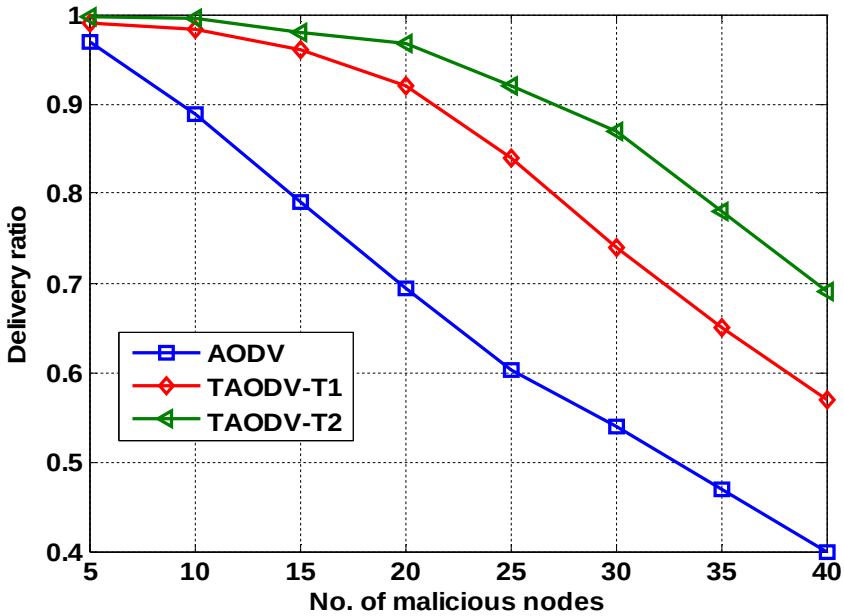


**Figure 4.7** **Delivery ratio of TAODV for different number of malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

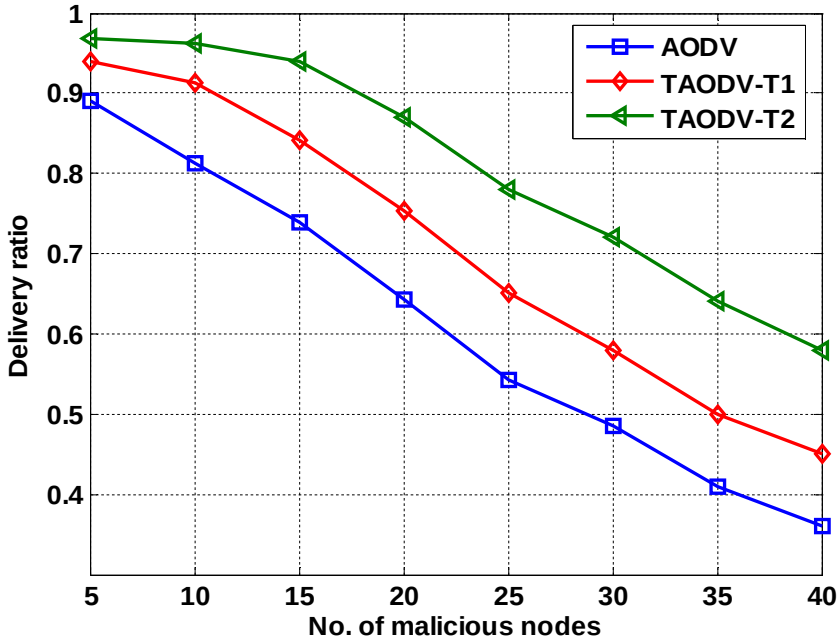


**Figure 4.8 Delivery ratio of TAODV for different number of malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

The delivery ratio of TAODV of 200 nodes is higher than that of TAODV of 150 nodes for different coverage areas which are proved through Figure 4.5 and Figure 4.7. Even though, the delivery ratio of TAODV is increased for more nodes, the delivery ratio of TAODV reduces for increased coverage areas (500×500 $m^2$) as shown in Figure 4.6 and Figure 4.8. The reason is that the nodes are more randomly scattered in coverage area of 500×500 $m^2$ than that of 300×300 $m^2$.

### 4.4.2 Routing Overhead

TAODV has an overall lower routing overhead compared to that of AODV which is revealed through the results illustrated by Figures 4.9 to 4.12. The routing overhead of TAODV is lesser by approximately 58% and 64 % than that of AODV for T1 and T2 levels respectively in case of 200 nodes with coverage area 300 × 300 $m^2$ shown in Figure 4.11. The reduced routing overhead is due to the increased forwarding rate and less number of control packets generated for each data packet transmitted by trusted route in TAODV.

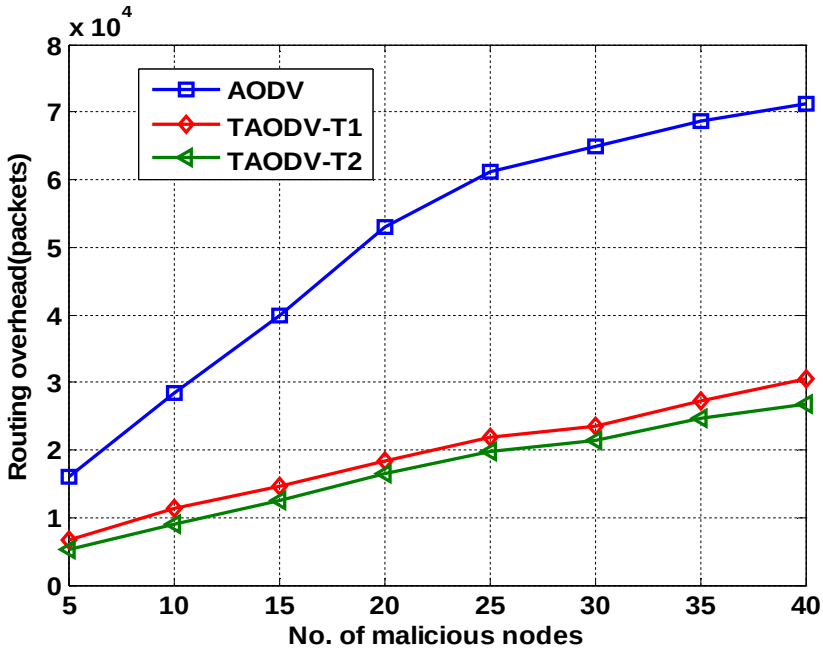


**Figure 4.9** **Routing overhead of TAODV with respect to malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

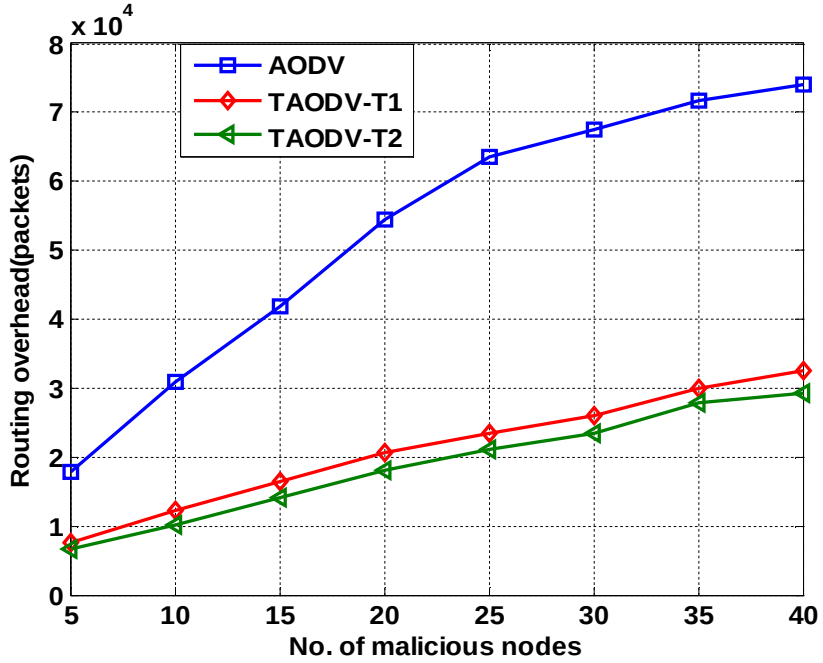


**Figure 4.10** **Routing overhead of TAODV with respect to malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

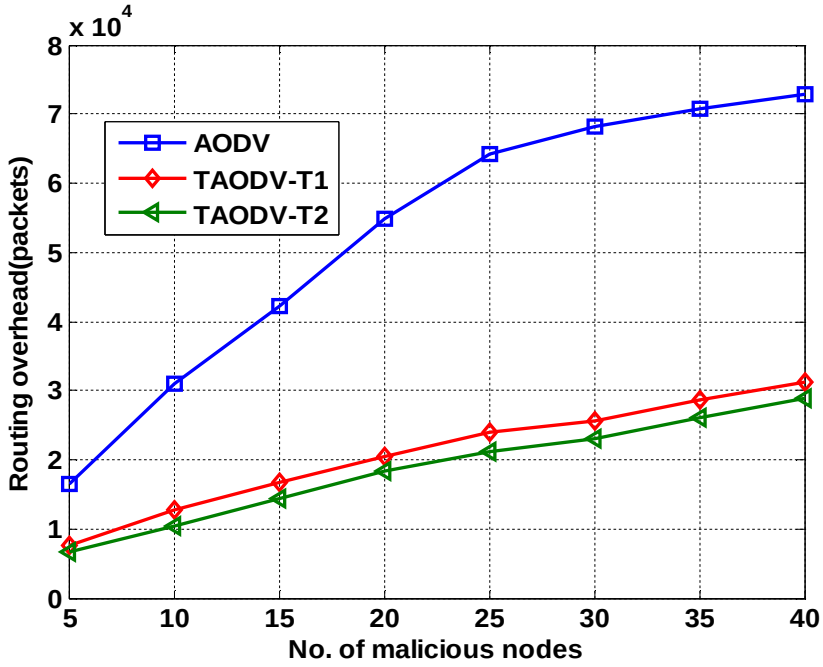


**Figure 4.11** **Routing overhead of TAODV with respect to malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

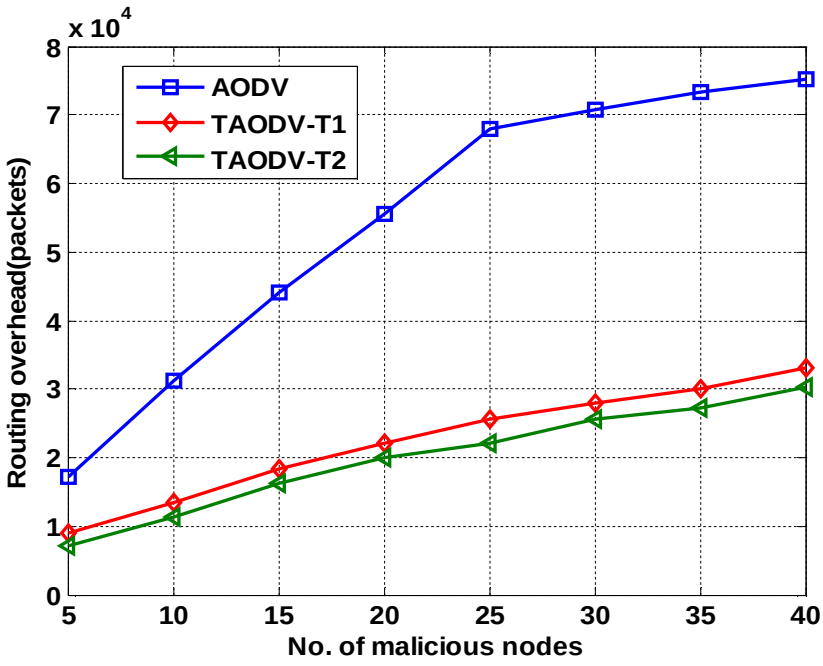


**Figure 4.12** **Routing overhead of TAODV with respect to malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

Although, TAODV has lesser routing overhead than that of AODV, higher routing overhead is obtained through TAODV for increased coverage area (500×500m$^2$) as shown in Figure 4.10 and Figure 4.12. This is due to the reduction in forwarding rate of packets from source to destination for coverage area of 500×500m$^2$ than that of 300×300m$^2$.

### 4.4.3 End to End Delay

From the simulation results (Figure 4.13 to Figure 4.16), it is observed that end to end delay of TAODV protocol is higher than that of AODV protocol. For increased malicious nodes, the delay of TAODV increases by approximately 5% and 8% than that of AODV protocol for T1 and T2 levels respectively when considering 200 nodes with coverage area 300×300m$^2$ as shown in Figure 4.15. The increment in the delay of TAODV is due to the additional time taken by the proposed scheme to identify the trusted path used to transfer the data to the required destination from the source node.

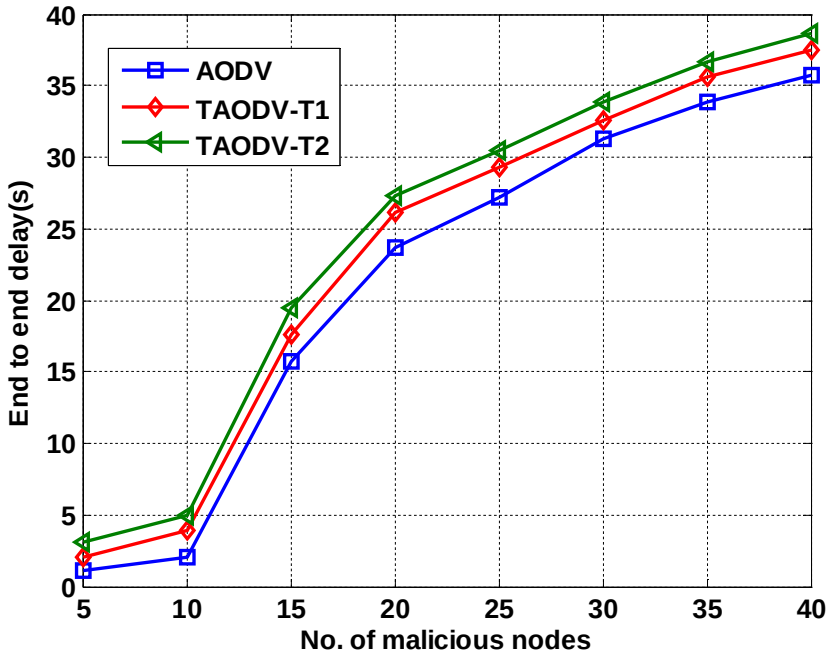


**Figure 4.13 End to end delay of TAODV for various malicious nodes for 150 nodes with coverage area 300×300 m$^2$**

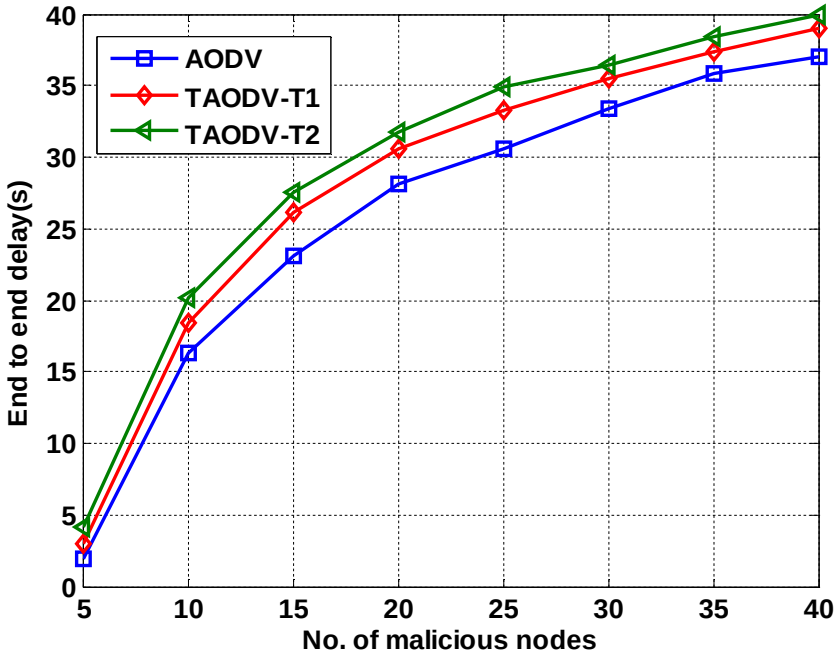


**Figure 4.14** **End to end delay of TAODV for various malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

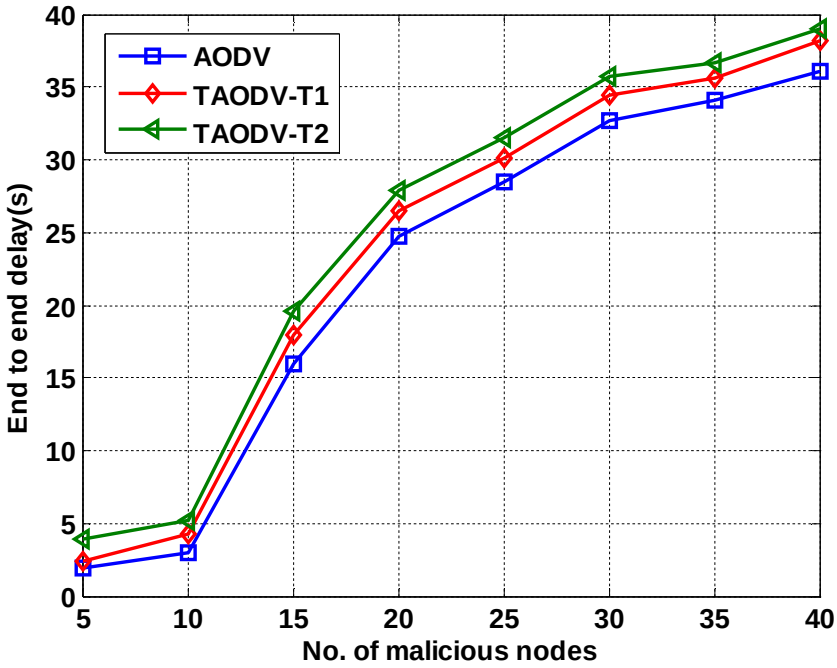


**Figure 4.15** **End to end delay of TAODV for various malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

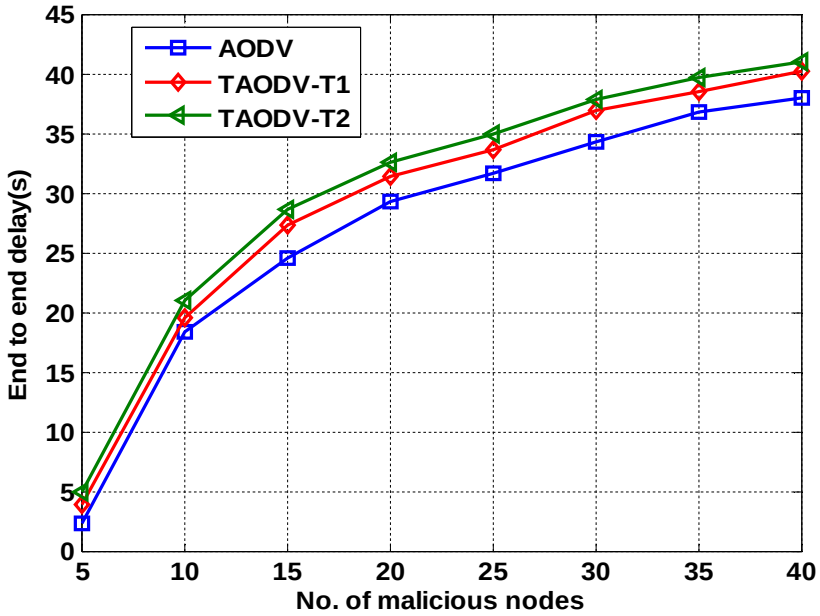


**Figure 4.16 End to end delay of TAODV for various malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

The delay of TAODV for coverage area of 500×500 $m^2$ (Figure 4.14 and Figure 4.16) is higher than that of 300×300 $m^2$ (Figure 4.13 and Figure 4.15) for 150 and 200 nodes. Larger delay obtained through TAODV is due to the more number of hops used by the TAODV for increased coverage area.

## 4.5 CONCLUSION

TAODV is implemented for mobile sensor networks with different coverage areas considering 150 and 200 nodes for two trust levels T1 and T2 respectively. It is compared with AODV protocol for different number of malicious nodes. The results show that, an improvement of 23% to 30% and 53% to 60% in the delivery ratio has been achieved in the TAODV protocol for trust levels T1 and T2 respectively than that of AODV protocol. Further more, the routing overhead achieved using the TAODV protocol (T2 level) was 65% less than the standard AODV protocol. The improvement in the above mentioned network performance is mainly due to trusted route and increased forwarding rate achieved through TAODV by implementing node trust and route trust in AODV to avoid the malicious nodes. However, the delay obtained using TAODV is higher than that of AODV which has to be abided for increased forwarding rate achieved through TAODV.

# CHAPTER 5

# TRUST BASED GREEDY PERIMETER STATELESS ROUTING PROTOCOL

## 5.1 INTRODUCTION

DSR and AODV are source based routing protocols in which the route is initiated by the source for routing the packets. These protocols do not utilise geographical position of the neighbour node closest to the destination to forward the packet. Greedy perimeter stateless routing (GPSR) is one such protocol that transmits the packets to the required target node by using the neighbour node having minimum distance with respect to the destination node which in turn enhances the performance of the network. However, the performance of GPSR is poor when the benevolent nodes are captured and compromised by malicious nodes. To improve the performance of wireless networks, trust based greedy perimeter stateless routing is developed by isolating the malevolent nodes. TGPSR is proposed for WSN by incorporating sensing module to the nodes along with trust based frame work in GPSR and is explained in this chapter. The network performance of TGPSR are analysed through simulation results and compared with GPSR.

## 5.2 GREEDY PERIMETER STATELESS ROUTING PROTOCOL

The greedy perimeter stateless routing is one of the commonly used location-based routing protocols in the sensor network. This protocol virtually operates in a stateless manner and has the ability for multi-path routing. In GPSR, it is assumed that all nodes recognise the geographical position of destination node with which communication is desired. This location information (i.e.) geographical position is also used to route traffic to its requisite destination from the source node

through the shortest path. Each transmitted data packet from the forwarding node contains the destination node's identification and its geographical position in the form of two four-byte float numbers. Each node also periodically transmits a beacon, to inform its adjacent nodes regarding its current geographical co-ordinates. The node positions are recorded, maintained and updated in a neighbourhood table by all nodes receiving the beacon. To reduce the overhead due to periodic beacons, the node positions are piggy-backed onto forwarded data packets. GPSR supports two mechanisms for forwarding data packets such as greedy forwarding and perimeter forwarding.

### 5.2.1 Greedy Forwarding

In greedy forwarding mechanism, nodes use the geographical position of the neighbours to forward the packets. The greedy forwarding mechanism is illustrated in Figure 5.1. Node 'i' receives a packet destined for destination say 'D'. The next neighbour node of i is identified by considering the radio range of i denoted by the dotted circle about the node i and the dashed arc with radius equal to the distance between the neighbour node say 'j' and D. Since the distance between the j and D is less than the distance between D and any of the node i's neighbours, then the node i forwards the packet to j. This greedy forwarding process repeats until the packet reaches D [92]. Since the forwarding is done on a packet to packet basis, it requires minimal state information to be retained by all nodes. This is most

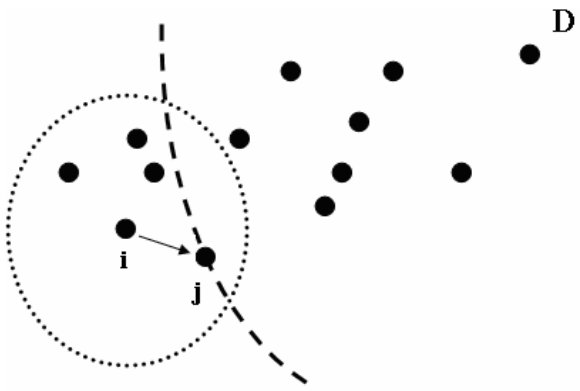


**Figure 5.1 Greedy forwarding mechanism**

suitable for resource starved devices. However, this mechanism is susceptible to failure in situations where the distance between forwarding node and final destination is less than the distance between the forwarding node's adjacent neighbours and destination.

### 5.2.2 Perimeter Forwarding

To overcome routing problems in such situations, GPSR engages perimeter forwarding mechanism. In this mechanism, the data packet is marked as perimeter mode along with the location where greedy forwarding failed. These perimeter mode packets are forwarded using simple planar graph traversal. Each node receiving a data packet marked as in perimeter mode uses the right-hand rule to forward packets to nodes, which are located counterclockwise to the line joining forwarding node and the destination. The perimeter forwarding mechanism is shown in Figure 5.2. Each node, while forwarding perimeter mode packets, compares its present distance to the destination from the point where greedy forwarding has failed. If the current distance is less, packet is routed through greedy forwarding repeatedly from that point onwards.

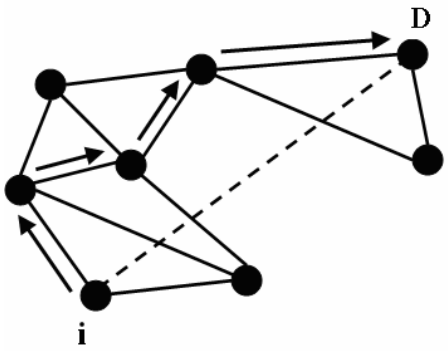


**Figure 5.2 Perimeter forwarding mechanism**

The protocol has been designed and developed based on the assumption that all nodes in the network executing this protocol are benevolent in nature. However, due to number of reasons including malice and incompetence, nodes frequently deviate from defined standards leading to routing predicaments. Hence, trust based greedy perimeter stateless routing [93] is developed for wireless networks by appending trust framework in the GPSR to get rid of malicious nodes.

## 5.3 TRUST BASED GREEDY PERIMETER STATELESS ROUTING PROTOCOL

GPSR scans its neighbourhood table to retrieve the next hop which is optimal and leads to the destination, during packet transmission to a known host. As there may be more than one such hop available, GPSR selects an adjacent neighbour that has the least distance to a particular destination. In contrast, the trust levels are incorporated in conjunction with the geographical distances in the neighbourhood table to create the most trusted route rather than the default minimal distance in TGPSR. The TGPSR for WSN is proposed by appending the sensing agent to the nodes along with the trust based model. In the TGPSR scheme, the accuracy and authenticity of immediate neighbouring nodes is ensured by observing their contribution to packet forwarding mechanism.

The trust mechanism is implemented by buffering the TUI [81] of each forwarded packet in the node as (GPSR Agent::buffer packet). After transmission, each node promiscuously listens for the neighbouring node to forward the packet. If the neighbour forwards the packet without any alteration within the TUI, its corresponding TLC is incremented which specifies the absence of malicious nodes. However, if the packet is modified by the neighbouring node in an unexpected manner or does not transmit the packet at all, its trust level is decremented which indicates that the node is identified as malicious node.

The transmitting node checks the different fields of the forwarded packet for requisite modification through a sequence of integrity checks (GPSR Agent::verify packet integrity). If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its DTM is incremented. On the other hand, if the integrity check fails or the forwarding node does not transmit the packet at all, then its corresponding direct trust measure is decremented so that the node is treated as malicious node. Then the forwarding node finds an alternate trustworthy neighbour node to forward the packet by isolating that neighbour node. This procedure is repeated until the last packet reaches the target node successfully. The TGPSR is explained by using flow chart as shown in Figure 5.3.

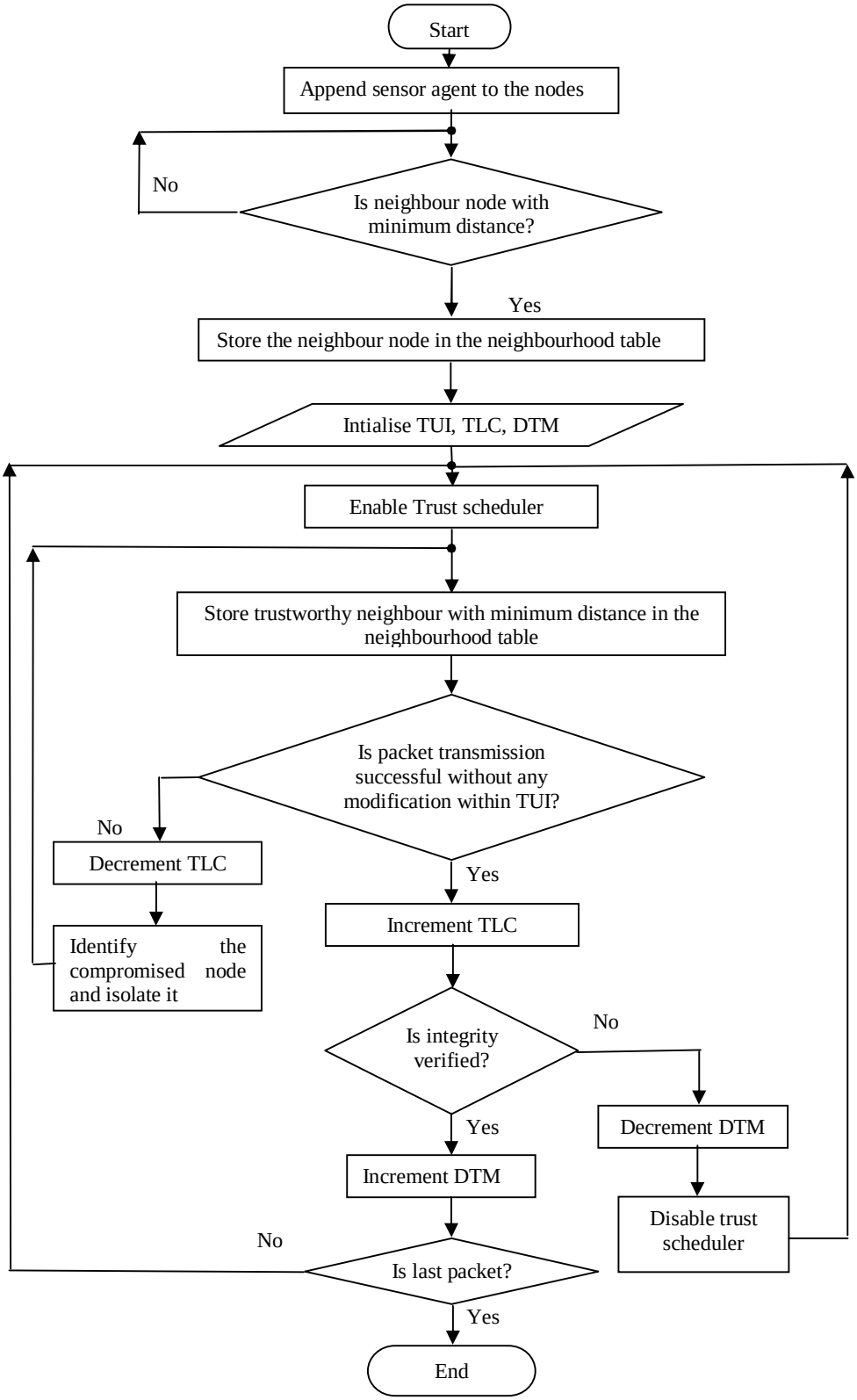


**Figure 5.3 Flowchart of TGPSR protocol**

## 5.4 SIMULATION RESULTS AND DISCUSSION

TGPSR protocol is obtained by implementing the trust and mobility model in the existing GPSR protocol. The simulation is done by using ns-2.32[97]. The NAM output for 150 nodes with 10 malicious nodes indicated in red circle is shown in Figure 5.4. The performance parameters such as delivery ratio, routing overhead and delay are calculated for 150 and 200 nodes by varying the number of malicious nodes from 5 to 40 with various coverage areas such as 300×300 $m^2$ and 500×500 $m^2$. The parameters used in the simulation are listed in Table 5.1.

**Table 5.1 Simulation parameters for TGPSR**

| Simulation Parameters | Values |
|---|---|
| Number of Nodes | 150 and 200 |
| Geographical area($m^2$) | 300×300and 500×500 |
| Packet Size(bytes) | 512 |
| Number of malicious nodes | 5 to 40 |
| Trust update interval(s) | 5 and 7 |
| Mobility model | Random way point |
| Pause time(s) | 20 |
| Simulation time(s) | 100 |

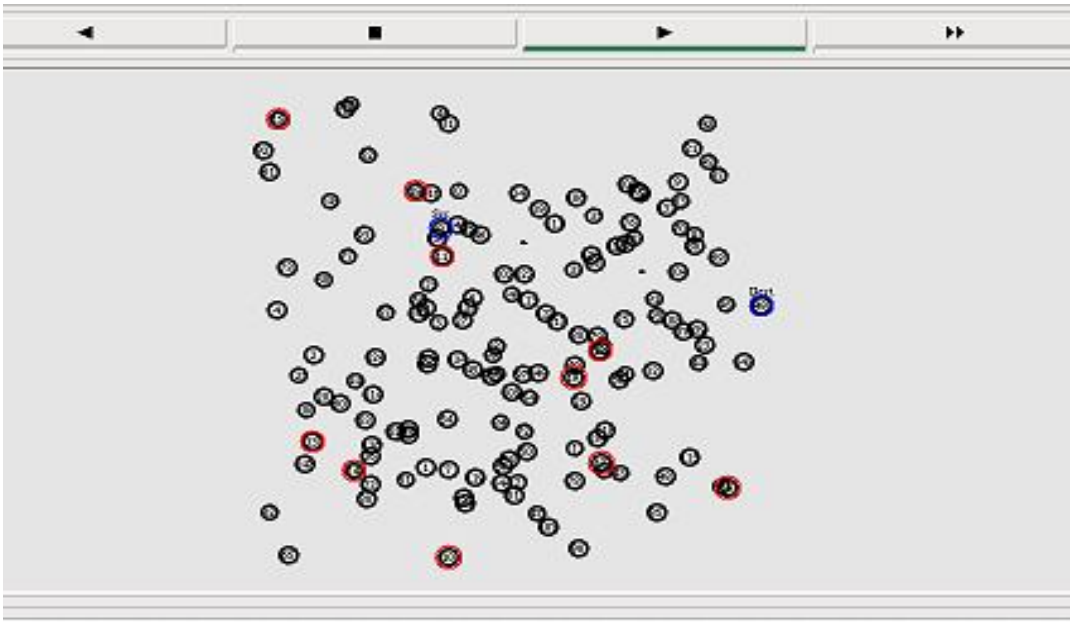

**Figure 5.4 NAM output of TGPSR for 150 nodes with ten malicious nodes**

### 5.4.1 Delivery Ratio

Delivery ratio of TGPSR is higher than that of GPSR for 150 and 200 nodes with different coverage area of 300×300 $m^2$ and 500×500 $m^2$ which is shown from Figure 5.5 to Figure 5.8. The delivery ratio of TGPSR is almost 98% for 5 to 15 malicious nodes for T2 level which is far better than GPSR illustrated by Figure 5.5. It is also observed from the same figure that the delivery ratio of TGPSR is nearly 34% and 63% greater than that of the GPSR for T1 and T2 levels respectively considering 20 malicious nodes for 150 nodes with coverage area 300×300$m^2$. For 200 nodes, TGPSR outperforms GPSR by providing delivery ratio of nearly 98% up to 20 malicious nodes for T2 level depicted in Figure 5.7.

The fact is that shorter and trusted routes are preferred for transmitting the packets from source to destination in TGPSR. Moreover, TGPSR selects or deselects the neighbour node for routing process based on their trust levels along with the minimum distance with respect to destination node to avoid the malicious node. Thus TGPSR improves the delivery ratio by increasing the forwarding rate.

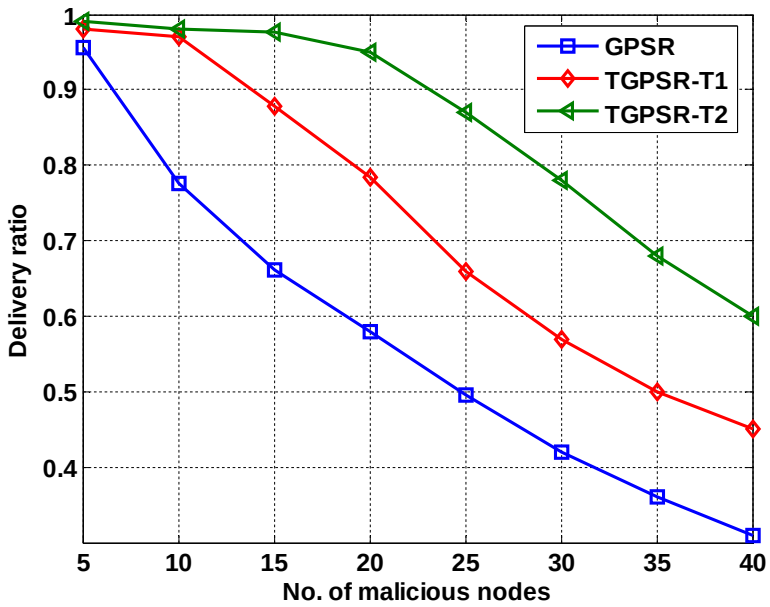


**Figure 5.5 Delivery ratio of TGPSR with respect to malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

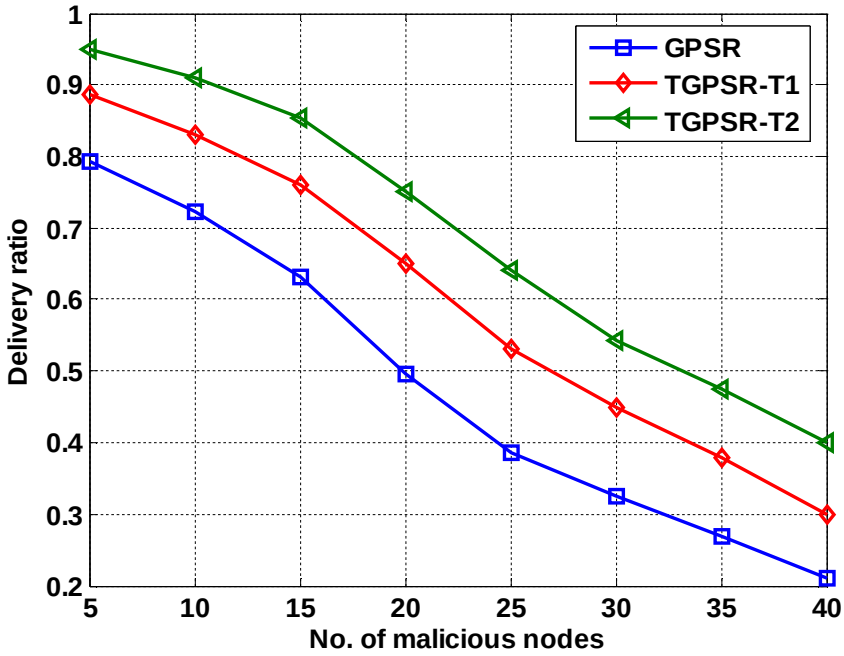


**Figure 5.6** **Delivery ratio of TGPSR with respect to malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

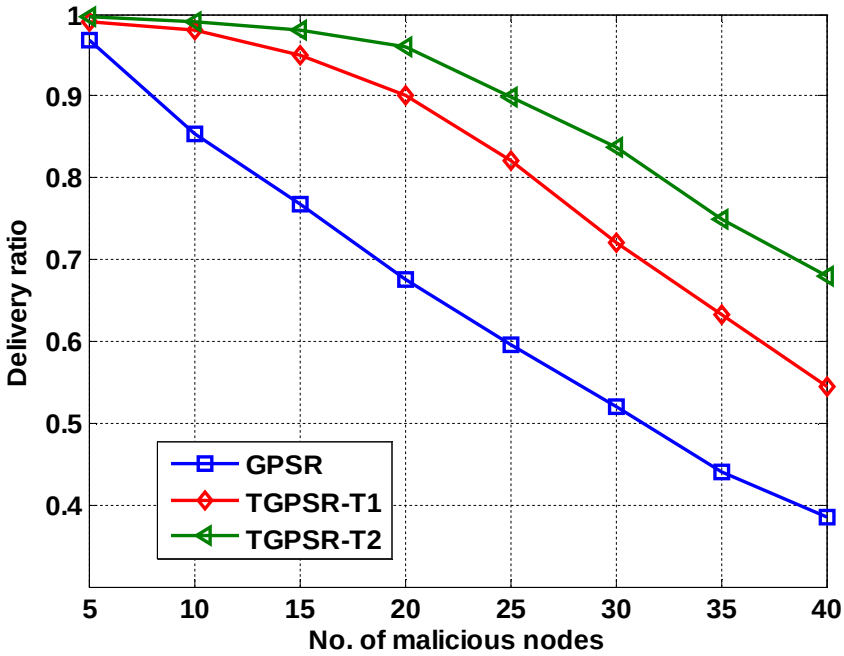


**Figure 5.7** **Delivery ratio of TGPSR with respect to malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

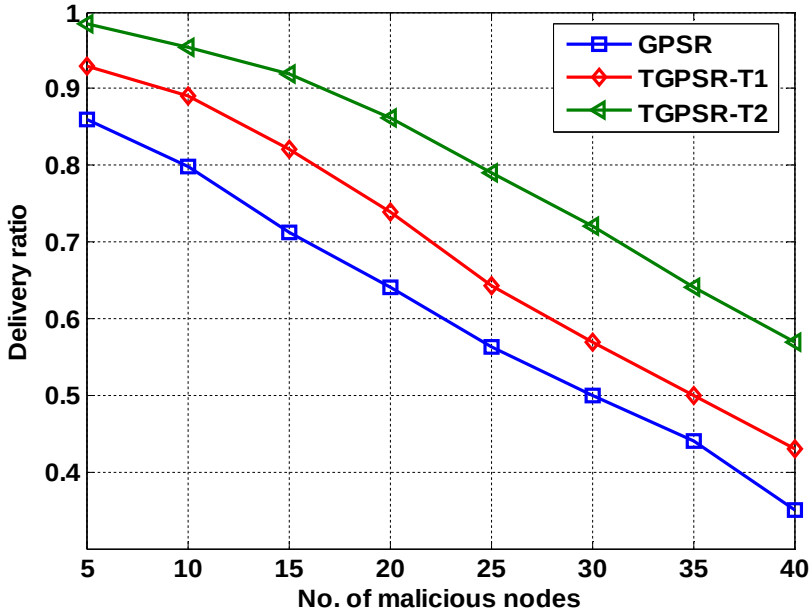


**Figure 5.8** **Delivery ratio of TGPSR with respect to malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

### 5.4.2 Routing Overhead

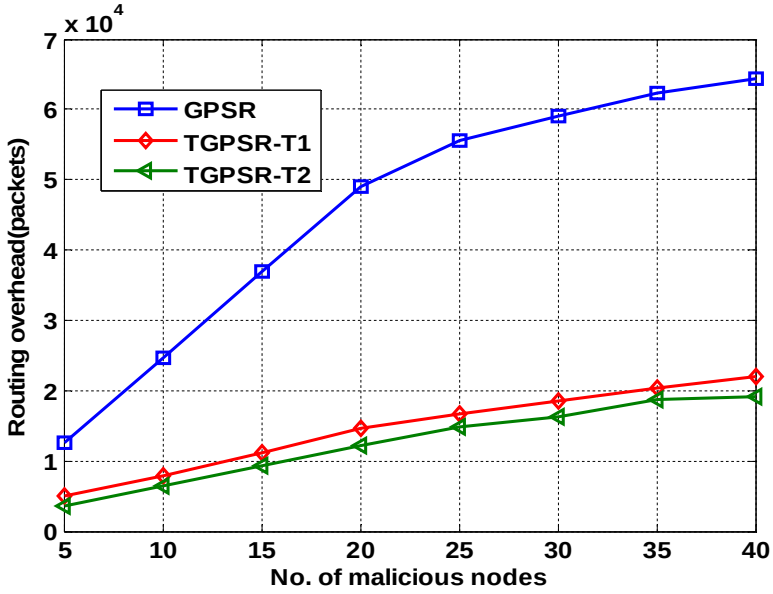


**Figure 5.9** **Routing overhead of TGPSR for various malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

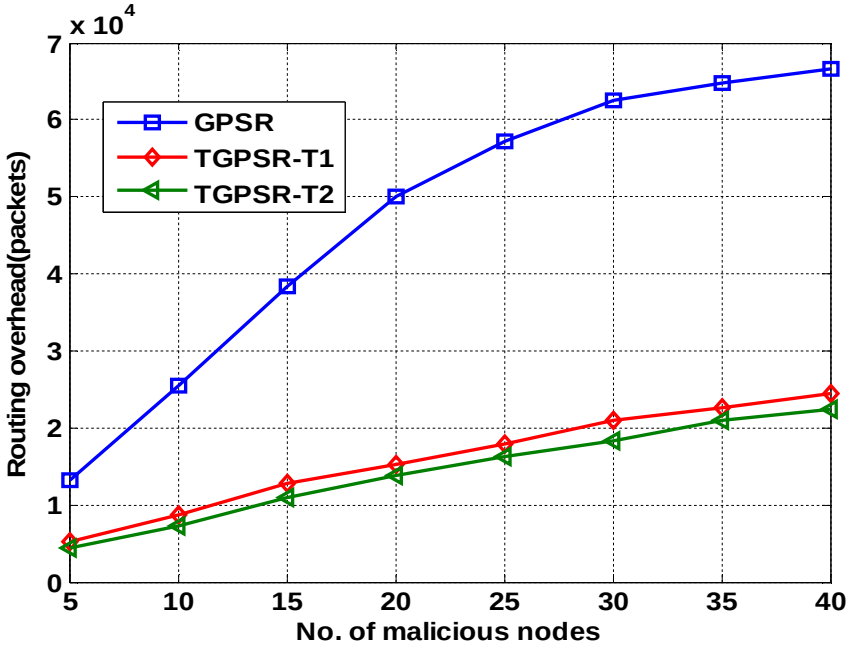


**Figure 5.10** **Routing overhead of TGPSR for various malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

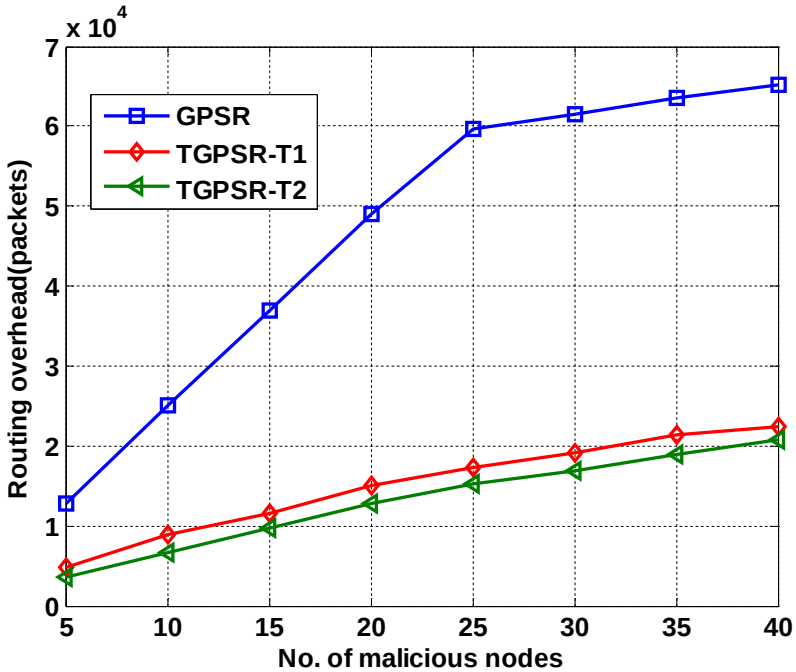


**Figure 5.11** **Routing overhead of TGPSR for various malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

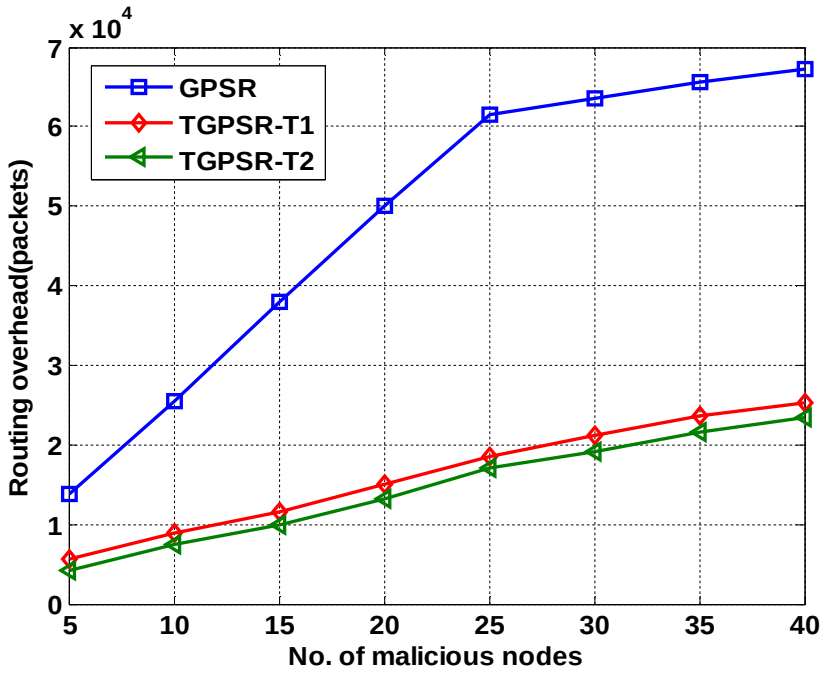


**Figure 5.12 Routing overhead of TGPSR for various malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

TGPSR achieves significant reduction in routing overhead compared to that of GPSR. This is illustrated through the simulation results revealed from Figure 5.9 to Figure 5.12. Though routing overhead of TGPSR and GPSR increases, for increased values of malicious nodes, TGPSR has lower routing overhead of nearly 65% and 70% for T1 and T2 levels respectively than that of GPSR in case of 150 nodes as shown in Figure 5.9. The reduced routing overhead is due to increased delivery ratio which reduces the number of control packets generated for each data packet in TGPSR.

However, the routing overhead of TGPSR increases for increased coverage area (500×500 $m^2$) in case of both 150 and 200 nodes as shown in Figure 5.10 and Figure 5.12. The increment in the routing overhead is due to reduced forwarding rate obtained through TGPSR for coverage area of 500×500 $m^2$ compared to that of 300×300 $m^2$.

### 5.4.3 End to End Delay

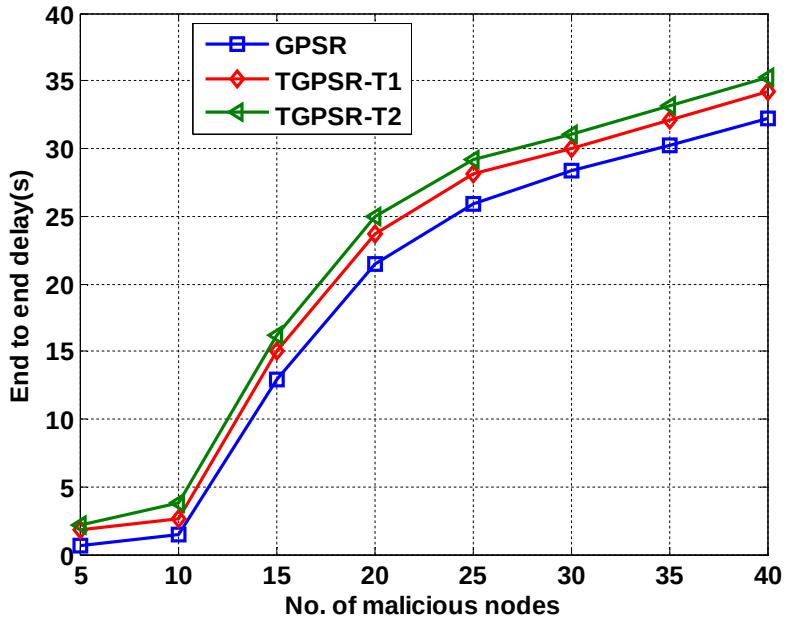


**Figure 5.13** **End to end delay of TGPSR with different number of malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

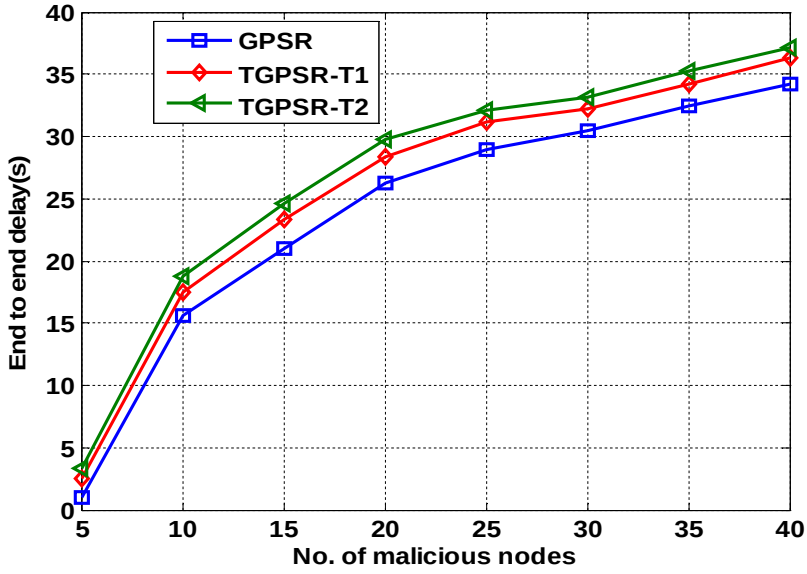


**Figure 5.14** **End to end delay of TGPSR with different number of malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

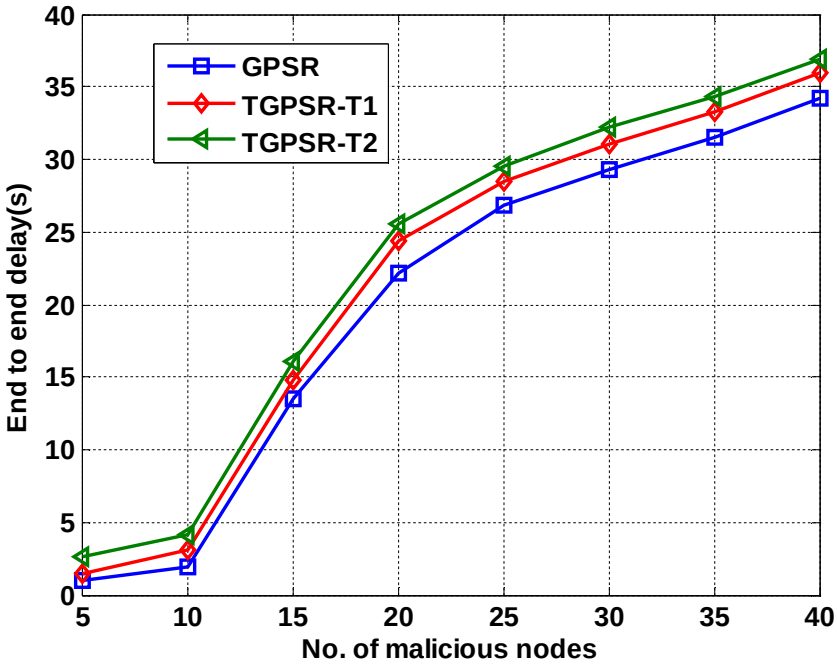


**Figure 5.15** **End to end delay of TGPSR with different number of malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

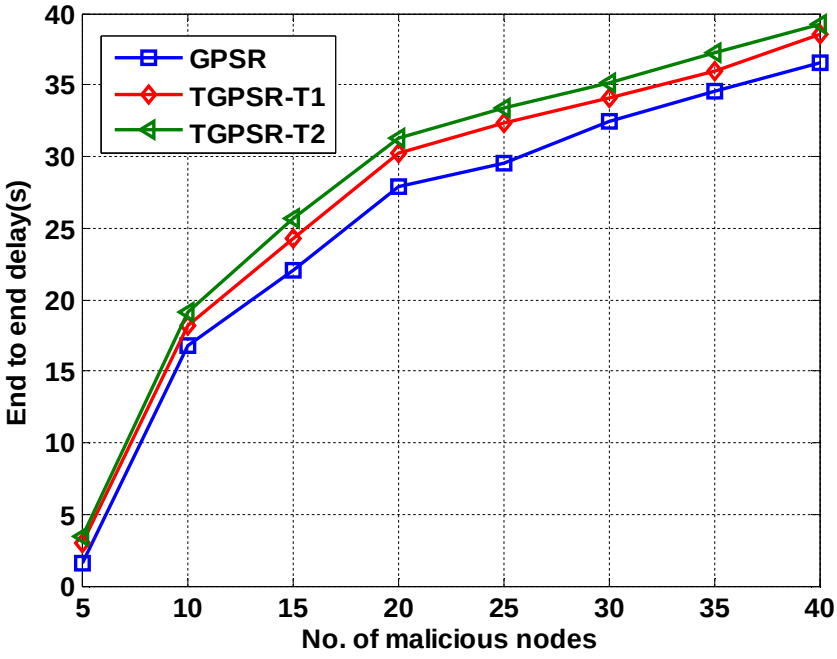


**Figure 5.16** **End to end delay of TGPSR with different number of malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

It is verified through simulation results shown in Figure 5.13 to Figure 5.16 that delay of TGPSR protocol is higher than that of GPSR protocol. When the number of malicious nodes is increased further, TGPSR increases the delay nearly by 6% and 8% for T1 and T2 levels respectively than that of GPSR protocol. TGPSR selects intermediate nodes based upon their trusted path in addition to the minimal distance from the destination.

The end to end delay of TGPSR of coverage area 500×500 $m^2$ is higher than the coverage area of 300×300$m^2$ demonstrated in Figure 5.14 and 5.16. The higher delay attained by TGPSR for larger coverage area is due to the more number of hops taken by trusted path to transfer the packets from source to target node in TGPSR.

## 5.5 CONCLUSION

TGPSR protocol is implemented for mobile sensor network with different coverage areas considering 150 and 200 number of nodes for simulation. It is compared with GPSR protocol for different number of malicious nodes. The results show that, an improvement of approximately 34 % and 63 % in the delivery ratio has been achieved in the TGPSR protocol for T1 and T2 levels respectively. Further more, the routing overhead achieved using the TGPSR protocol was about 65% and 70% less than the standard GPSR protocol for T1 and T2 levels respectively. However, the delay obtained through TGPSR is higher than that of GPSR which has to be tolerated for increased delivery ratio and reduced routing overhead. The improvement in the performance such as delivery ratio and routing overhead is mainly due to trust based model implemented in GPSR and less number of control packets taken by the TGPSR to get rid of the attackers.

# CHAPTER 6

# TRUST BASED ENERGY AWARE GREEDY PERIMETER STATELESS ROUTING PROTOCOL

## 6.1 INTRODUCTION

Routing of packets in the GPSR protocol is based only on the path using the nodes having minimum distance from destination. This consideration of single metric makes this protocol to use the same set of nodes repeatedly which in turn results in battery power exhaustion of the nodes. Then the path using those nodes breaks down quickly resulting in poor network connectivity. Hence, energy level of nodes is also considered as another metric along with the minimum distance to develop energy aware greedy perimeter stateless routing (EGPSR) and improve the network connectivity and performance. However the network performance of EGPSR will be degraded when the nodes are compromised by attackers. Therefore, trust based energy aware greedy perimeter stateless routing (TEGPSR) is developed to avoid the malevolent nodes and is described in this chapter. The performance of TEGPSR is analysed through simulation results and compared with EGPSR.

## 6.2 ENERGY AWARE GREEDY PERIMETER STATELESS ROUTING PROTOCOL

In EGPSR algorithm, each node broadcasts HELLO packets to all its neighbours that are in its communication range [94]. The HELLO packet contains the location information of the node, rate of energy consumption and fraction of energy consumption [95]. The rate of energy consumption ($R_{in}$) of $i^{th}$ node after $n^{th}$ periodic interval is calculated by equation (6.1)

$$R_{in} = \frac{(E_{i0} - E_{in})}{(n-1)H_p} \quad . \tag{6.1}$$

where, $E_{i0}$ is the initial energy of the $i^{th}$ node.

$E_{in}$ is energy of $i^{th}$ node at the start of the $n^{th}$ periodic interval.

$H_p$ is the HELLO period.

Then the fraction of energy consumption ($F_{in}$) of $i^{th}$ node after $n^{th}$ periodic interval is also calculated by equation (6.2).

$$F_{in} = \frac{E_{i0} - E_{in}}{E_{i0}} \tag{6.2}$$

The node also maintains the table of its direct neighbours to forward packets to the required destination. Each row of the table contains following information of a neighbour node such as, IDentification number (ID), geographical location, rate of energy consumption and fraction of energy consumption. The node updates the information of the neighbour after receiving the HELLO packet from the neighbour, if neighbour ID is already present in table. Otherwise, it adds the details of neighbour in the neighbourhood table, if the node is a new neighbour. The rate of energy consumption and fraction of energy consumption are used to determine the energy level needed for neighbour node to transmit the packet in EGPSR scheme. The adjacent neighbour which has minimum energy level requirement and least distance to a particular destination for forwarding the packet is selected from node's neighbourhood table in EGPSR [96]. This procedure is continued until the packet reaches the destination.

Eventhough EGPSR achieves enhanced network performance in terms of delivery ratio, it has poor forwarding rate in the presence of malevolent nodes. To obtain improved network performance, TEGPSR is proposed for WSN by isolating the compromised nodes.

## 6.3 TRUST BASED ENERGY AWARE GREEDY PERIMETER STATELESS ROUTING PROTOCOL

In TEGPSR, the trusted route for forwarding the packet is created by providing the trust levels along with the geographical distances and energy level in the neighbourhood table. The accuracy and trustworthiness of immediate neighbouring node is measured by monitoring its contribution in packet forwarding.

TUI of each forwarded packet is buffered in the node as (EGPSR Agent::buffer packet) to implement the trust mechanism. Each node after transmitting the packet promiscuously listens for the neighbouring node to forward the packet. If neighbour transmits the packet without any variation within the TUI, its corresponding TLC is incremented. However, if the neighbouring node alters the packet in an unpredicted manner or does not transmit the packet at all within the TUI, its trust level counter is decremented. Then that particular neighbour node is identified as malicious node.

The sending node also verifies the different fields of the forwarded packet for requisite modifications through a sequence of integrity checks as (EGPSR Agent::verify packet integrity). If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its direct trust measure, is incremented. On the other hand, if the integrity check fails or the forwarding node does not transmit the packet within the TUI, then its corresponding DTM is decremented and the neighbour node is detected as malicious node. Then that node is isolated and transmitting node finds an alternate trustworthy neighbour node to forward the packet. This process is repeated until the last packet reaches the destination. The flow chart of EGPSR is shown in Figure 6.1.

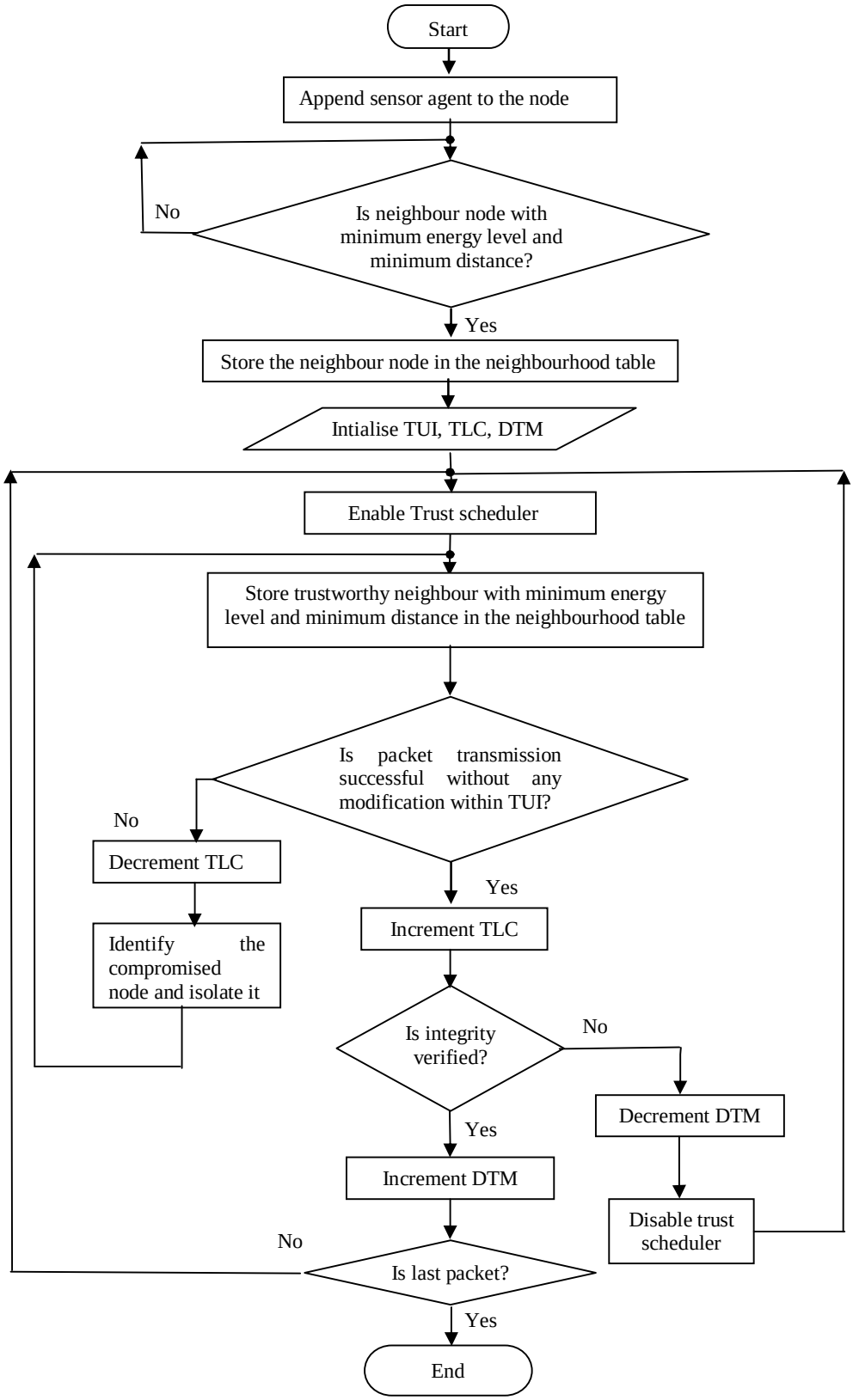


**Figure 6.1 Flowchart of TEGPSR protocol**

## 6.4 SIMULATION RESULTS AND DISCUSSION

The trust and mobility model is implemented in the existing EGPSR protocol to obtain the TEGPSR protocol. The TEGPSR protocol is simulated to emulate compromised nodes in the mobile sensor networks using ns-2.32 [97]. The performance parameters such as delivery ratio, routing overhead and delay are calculated for 150 and 200 nodes by varying the number of malicious nodes from 5 to 40 with various coverage areas such as 300×300 $m^2$ and 500×500 $m^2$. The NAM output of TEGPSR with attackers is shown in Figure 6.2. The parameters used in the simulation are listed in Table 6.1.

**Table 6.1 Simulation parameters for TEGPSR**

| **Simulation parameters** | **Values** |
|---|---|
| Number of nodes | 150 and 200 |
| Geographical area($m^2$) | 300×300, 500×500 |
| Packet Size(bytes) | 512 |
| Number of malicious nodes | 5 to 40 |
| Mobility model | Random way point |
| Pause time(s) | 20 |
| Trust update interval (s) | 5 and 7 |
| Simulation time(s) | 100 |

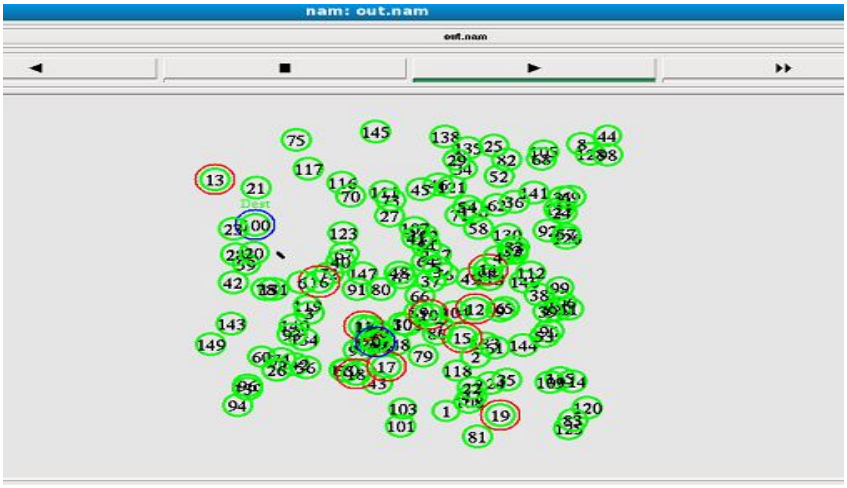


**Figure 6.2 NAM output of TEGPSR for 150 nodes with ten malicious nodes**

### 6.4.1 Delivery Ratio

TEGPSR outperforms EGPSR by achieving higher delivery ratio for different coverage areas of 300×300m$^2$ and 500×500 m$^2$ with 150 and 200 nodes as illustrated by the Figure 6.3 to Figure 6.6. Figure 6.3 depicts that the delivery ratio of TEGPSR for T2 level is almost 98% for 5 to 15 malicious nodes. It is also observed from the same figure that TEGPSR provides higher delivery ratio of about 16 % and 35 % for T1 and T2 respectively than that of EGPSR. Figure 6.5 describes that the delivery ratio remains almost 98% upto 20 malicious nodes for T2 level of TEGPSR.

The improvement in the delivery ratio of TEGPSR is due to the fact that TEGPSR selects the neighbour node for routing process based on trusted path along with minimum geographical distance and energy levels to get rid off the malicious nodes.

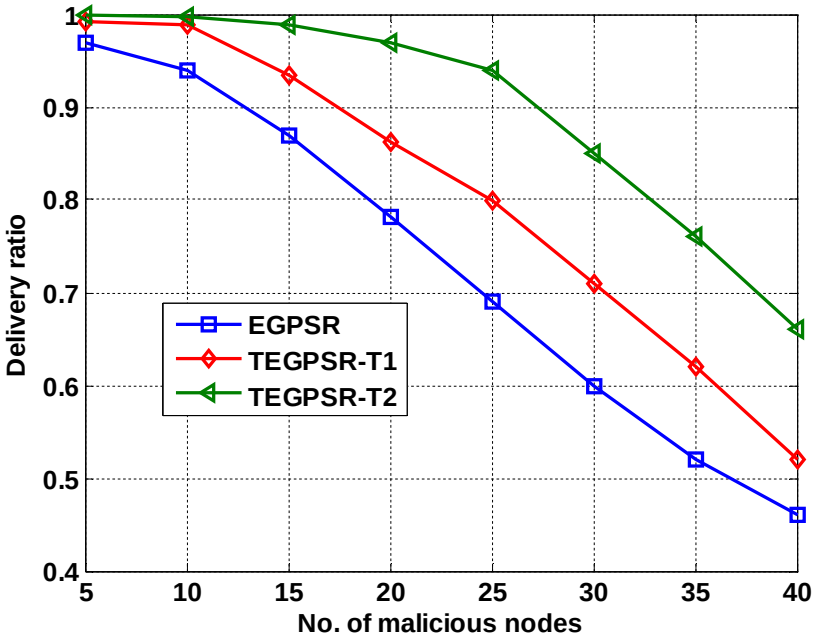


**Figure 6.3** **Delivery ratio of TEGPSR with respect to malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

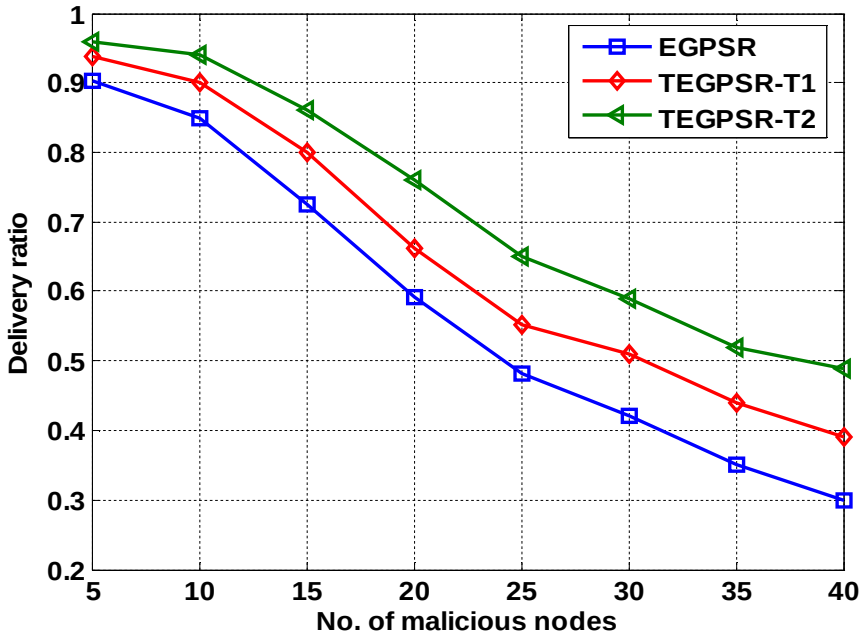


**Figure 6.4** **Delivery ratio of TEGPSR with respect to malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

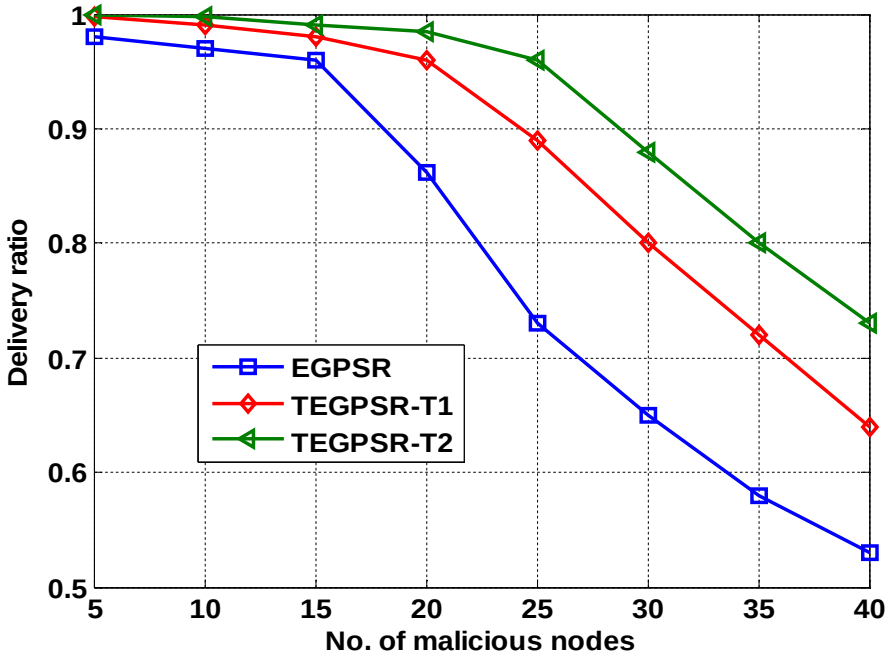


**Figure 6.5** **Delivery ratio of TEGPSR with respect to malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

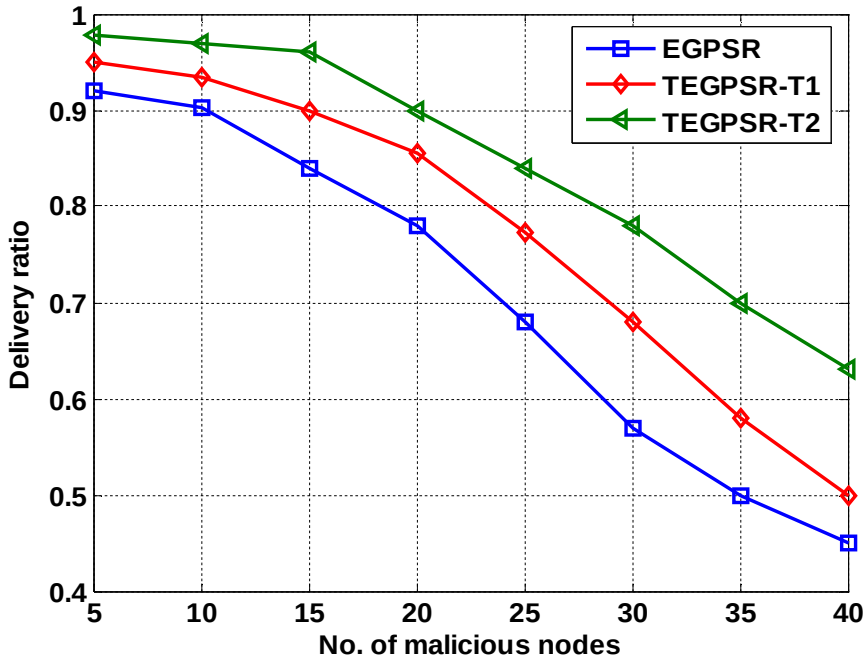


**Figure 6.6** **Delivery ratio of TEGPSR with respect to malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

### 6.4.2 Routing Overhead

Simulation results shown in Figure 6.7 to Figure 6.10 demonstrate that TEGPSR achieves significant reduction in routing overhead compared to that of EGPSR. For increased values of malicious nodes, TEGPSR has lower routing overhead of approximately 68% and 72% for T1 and T2 levels respectively than that of EGPSR depicted in Figure 6.7. The reduction in routing overhead achieved through TEGPSR is due to the less number of control packets generated by TEGPSR.

The routing overhead of TEGPSR is increased for larger coverage area of 500×500m$^2$ in case of both 150 and 200 nodes which is observed from the simulation results described in Figure 6.8 and Figure 6.10. The increased routing overhead is due to the reduced forwarding rate obtained through TEGPSR for coverage area of 500×500 m$^2$ compared to that of 300×300m$^2$.

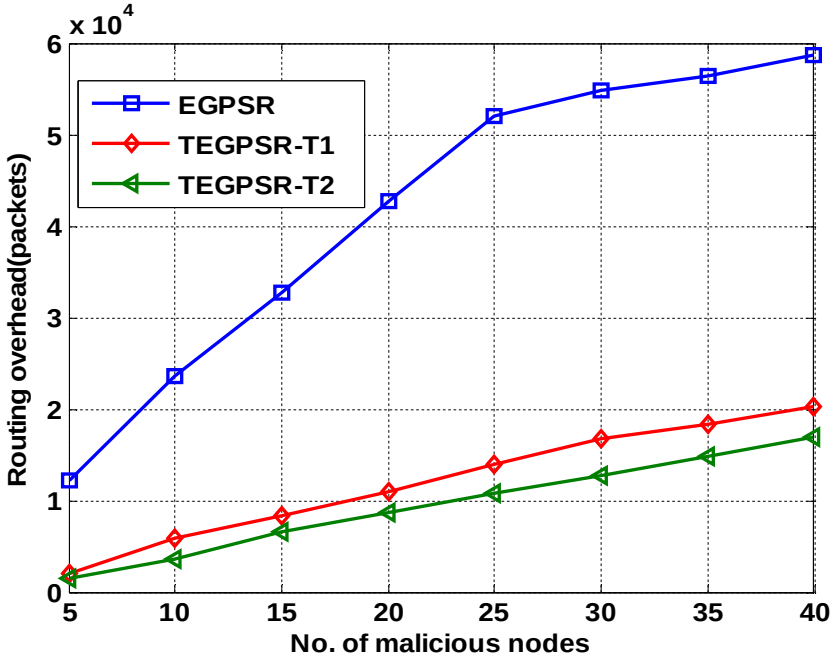


**Figure 6.7 Routing overhead of TEGPSR for various malicious nodes for 150 nodes with coverage area 300×300 m$^2$**

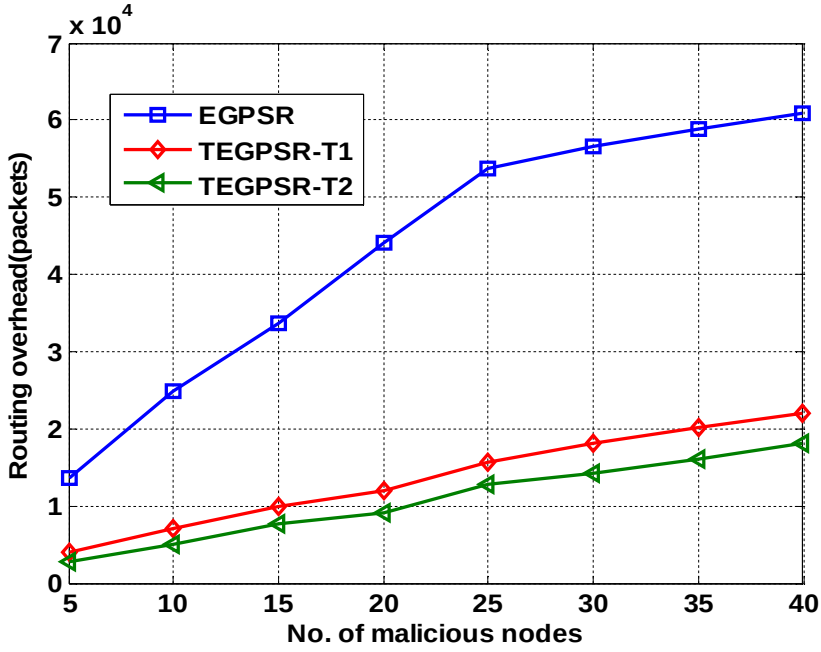


**Figure 6.8** **Routing overhead of TEGPSR for various malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

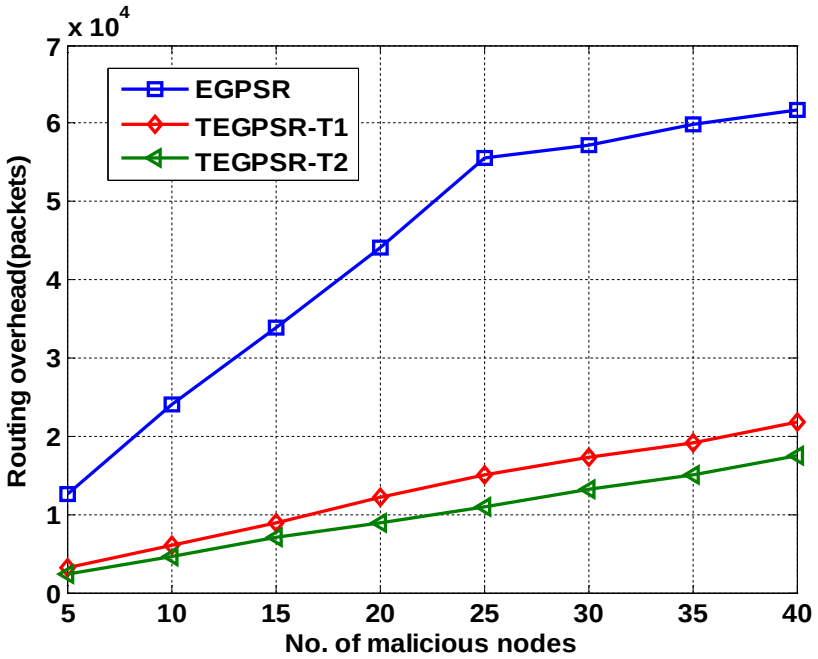


**Figure 6.9** **Routing overhead of TEGPSR for various malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

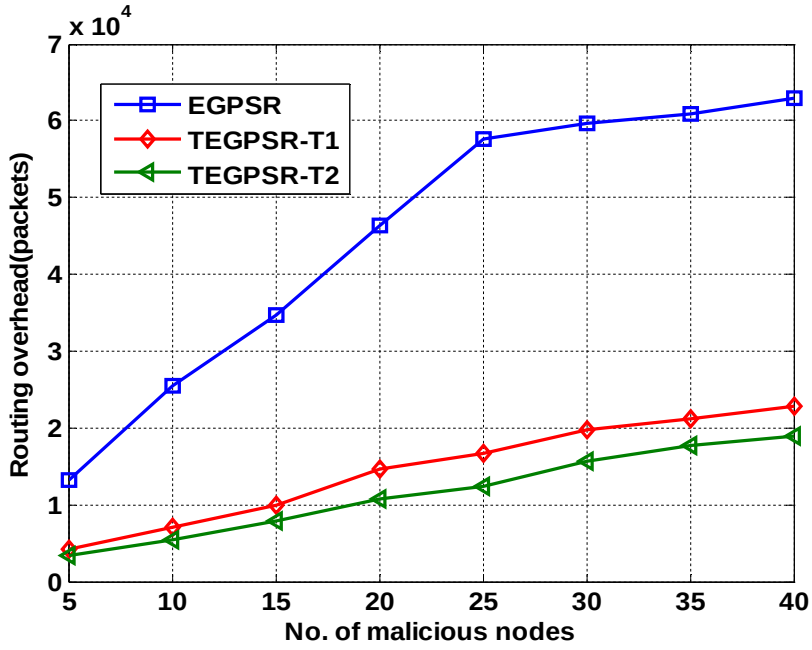


**Figure 6.10 Routing overhead of TEGPSR for various malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

### 6.4.3 End to End Delay

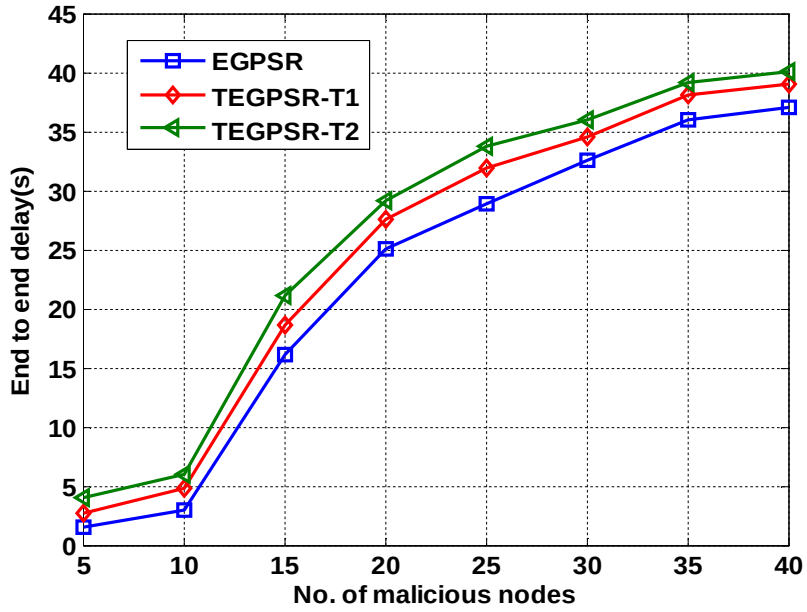


**Figure 6.11 End to end delay of TEGPSR for different number of malicious nodes for 150 nodes with coverage area 300×300 $m^2$**

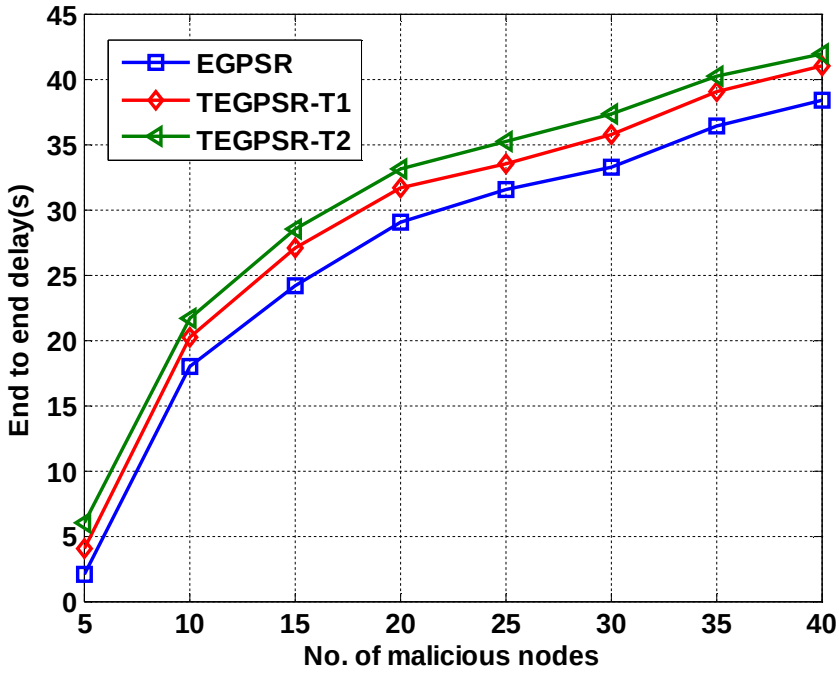


**Figure 6.12** **End to end delay of TEGPSR for different number of malicious nodes for 150 nodes with coverage area 500×500 $m^2$**

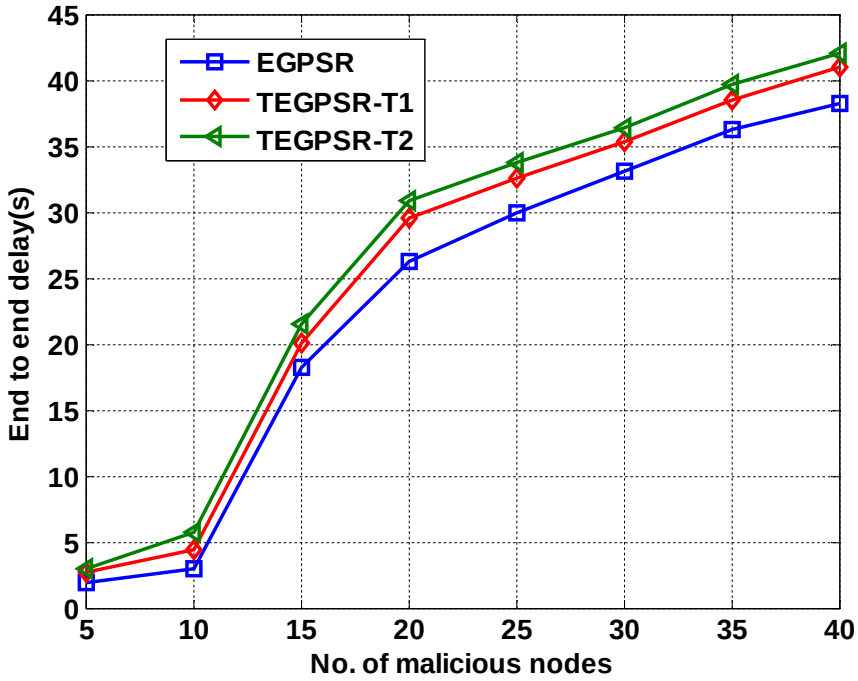


**Figure 6.13** **End to end delay of TEGPSR for different number of malicious nodes for 200 nodes with coverage area 300×300 $m^2$**

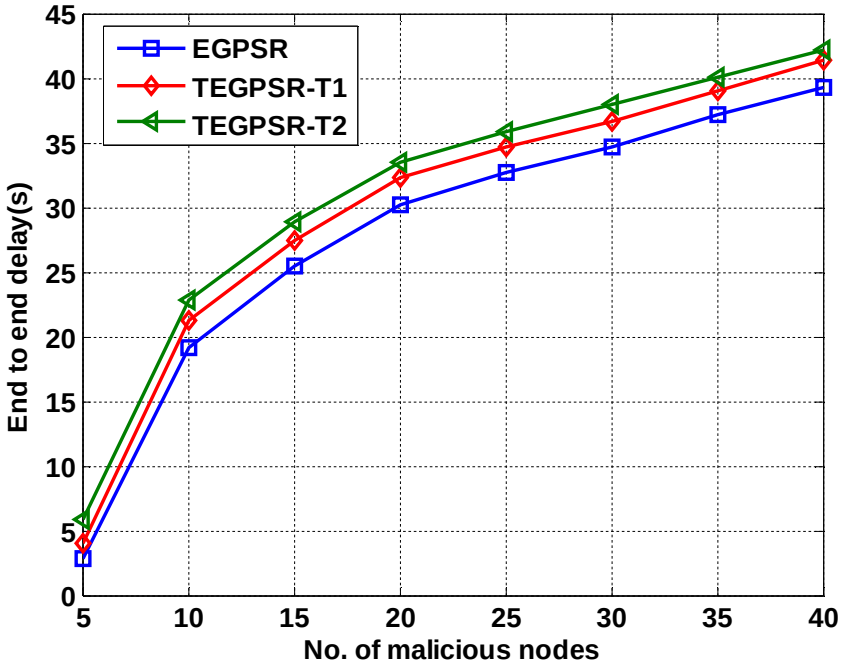


**Figure 6.14 End to end delay of TEGPSR for different number of malicious nodes for 200 nodes with coverage area 500×500 $m^2$**

Figure 6.11 to Figure 6.14 illustrate the performance of end to end delay with respect to malicious nodes for TEGPSR having two trust levels (T1 and T2) and EGPSR**.** The results portray that the higher end to end delay is obtained through TEGPSR than that of EGPSR. It is vivid through the result shown in Figure 6.11 that the delay of TEGPSR increases approximately 6.5 % and 9.5% for T1 and T2 respectively than that of EGPSR. The increment in the delay is due to the additional delay taken to identify the path using trusted route, minimum geographical distance with respect to target node and nodes having minimum energy level for transmission of packets from source to destination node.

Figure 6.12 and Figure 6.14 depict that the delay of TEGPSR is increased for increased coverage area (500×500 $m^2$). The higher delay is due to scattering of the nodes in more random manner and requirement of more hops to reach the destination in forwarding the packets in the coverage area of 500×500$m^2$ than that of 300×300 $m^2$.

## 6.5 CONCLUSION

TEGPSR protocol with T1 and T2 trust levels is implemented for mobile sensor network with different coverage area considering 150 and 200 nodes for simulation. It is compared with EGPSR protocol for different number of malicious nodes varying from 5 to 40. The results show that on the average, an improvement of about 33% in the delivery ratio has been achieved in the TEGPSR protocol for T2 level compared to that of EGPSR protocol. Further more, routing overhead achieved using the TEGPSR protocol was about 68% and 72% less than that of the standard EGPSR protocol for T1 and T2 levels respectively. However, an increment of approximately 6.5% and 9.5 % in delay for T1 and T2 levels respectively is obtained through TEGPSR compared to that of EGPSR protocol which is a permissible factor when considering the improved forwarding rate and reduced control packets. The improvement in the delivery ratio and routing overhead is mainly due to trusted routing decisions along with minimum energy level and distance with respect to destination and less number of control packets chosen by TEGPSR protocol to evade malicious nodes.

# CHAPTER 7

# SUMMARY AND CONCLUSIONS

## 7.1 GENERAL

An attempt has been made in the present work to enhance the performance of WSN in the presence of compromised nodes through trust based security framework incorporated in various routing protocols of WSN such as DSR, AODV, GPSR and EGPSR. The summary, salient conclusions and scope for further research work are presented in this chapter.

## 7.2 SUMMARY

The sensing technology combined with the advancement in electronics and wireless communication makes WSN lucrative and attractive for being exploited in abundance in civilian and military applications. The inclusion of wireless communication technology and deployment of sensor nodes ubiquitously in harsh environment in such applications incur various types of security threats. Providing security and privacy against these threats is a challenging issue in sensor networks due to limited capabilities of sensor nodes. Various secured routing protocols developed for WSN by appending cryptographic techniques in the routing protocols such as DSR, AODV, GPSR and EGPSR to protect network against attackers require extra processing, overhead and memory. Moreover, these secured routing methods have poor network performance.

An attempt has been made in the present work to develop trust based secured routing protocols by using the existing resources to improve network performance. Trust based routing protocols such as TDSR, TAODV, TGPSR and TEGPSR are simulated by varying the malicious nodes from 5 to 40 for different

coverage areas such as $300\times300m^2$ and $500\times500m^2$ with 150 and 200 nodes using *ns-2*. TDSR is developed to address the security mechanism by adopting trusted routing schemes along with the source route header information to protect the network from malicious nodes. Subsequently, TAODV is propounded by using trust based routing decisions to improve the forwarding rate of the packets by isolating the compromised nodes. Further, TGPSR is proposed by appending trusted path along with the geographical position of neighbour node with respect to the destination to elude the attackers and improve the network performance. Also, TEGPSR is implemented by integrating trust based security model in addition with the energy levels and distance to avoid the malevolent nodes and reduce the packet loss and control packets.

## 7.3 CONCLUSIONS

TDSR is anticipated for sensor networks by incorporating trust based model in the source based DSR protocol considering T1 (trust update interval of 5s) and T2 (trust update interval of 7s) trust levels. Simulation results demonstrate that TDSR achieves significant improvement in delivery ratio and reduction in overhead for trust levels T1 and T2 than that of DSR. However, end-to-end delay is higher in TDSR.

Node trust and route trust are integrated in the reactive AODV routing protocol to develop TAODV having two trust levels (T1 and T2) to evade the nodes compromised by malevolent nodes. TAODV outperforms the AODV in terms of increased delivery ratio by about 28 % and 53% approximately for trust levels T1 and T2 respectively. The higher routing overhead is the major constraint in TAODV.

TGPSR is proposed for the security enhancement of WSN with the incorporation of trust level along with shortest route information with respect to destination in the GPSR protocol by considering two trust levels (T1 and T2) to counteract the compromised nodes. The simulation results show that the TGPSR reduces routing overhead by around 65% and 70% for the trust levels T1 and T2

respectively. Also, it is evident that TGPSR significantly enhances the performance of WSN than GPSR by isolating the compromised nodes.

TEGPSR with two trust levels (T1 and T2) is propounded by integrating trust based routing decisions in EGPSR to avoid malicious nodes. Simulation results indicate that TEGPSR accomplishes significant reduction in terms of routing overhead by about 68% and 72% for trust level T1 and T2 respectively than EGPSR.

## 7.4 SCOPE FOR FUTURE WORK

The following are some of the potential problems that might be interesting for researchers to pursue and explore in future.

- The effects of trust schemes in hierarchical based routing protocols against the various security threats of WSN can be studied to achieve the security and performance enhancement (energy consumption) of the network.

- The security model using trust based framework for heterogeneous sensor network having two types of nodes with two different levels of energies against different types of attacks can be explored.

- The trust based security techniques pertaining to attacks of application and transport layer of WSN can be investigated.

- Efforts can be made to improve the performance of system by analyzing the WSN with security mechanisms for different types of services in the presence of compromised nodes.

- The real time implementation of the network using Zigbee hardware module with the incorporation of security mechanism can be worth exploring.

# REFERENCES


[1] Q.Bi, G.I.Zysman and H.Menkes, "Wireless mobile communications at the start of the 21st century", *IEEE Communications Magazine*, vol.39, no.1, pp.110-116, January 2001.

[2] Kaveh Pahlavan and Prashant Krishnamurthy, "*Principles of wireless sensor networks*", Prentice Hall, New Delhi, 2007.

[3] Erdal Cayirci and Chunming Rong, "*Security in wireless adhoc and sensor networks*", John Wiley and Sons Publications, United Kingdom, 2009.

[4] Mohammed Ilyas and Imad Mahgoub, "*Handbook of sensor networks: Compact wireless and wired sensing systems*", CRC Press, Washington, 2005.

[5] Sophia Kapantzis, "Security models for wireless sensor networks", *Research Report, Department of Electrical and Computer Systems Engineering*, Monach University, Melbourne, Australia, March 2006.

[6] I.F.Akyildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci, "A survey on sensor networks", *IEEE Communication Magazine*, vol.40, no.8, pp.102-114, August 2002.

[7] Jamal N.Al-Karaki and Ahmed E.Kamal, "Routing techniques in wireless sensor networks: A survey", *IEEE Transactions on Wireless Communication*, vol. 11, no.6, pp.6-28, December 2004.

[8] C.Karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, pp.113-127, May 2003.

[9] A.Perrig, J.Stankovic and D.Wagner, "Security in wireless sensor networks", *Communications of the ACM*, vol. 47, no. 6, pp.53-57, June 2004.

[10] Yong Wang, Garhan Attebury and Byrav Ramamurthy, "A survey of security issues in wireless sensor networks", *IEEE Communications Survey and Tutorials*, vol. 8, no.2, pp.2-23, Second Quarter 2006.

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, "Security in wireless sensor networks: Issues and challenges", *Proceedings of IEEE 8th International Conference on Advanced Communication Technology*, Korea, pp.1043-1048, February 2006.

[12] K.Jones, A.Wadaa, S.Olariu, L.Wilson and M.Eltoweissy, "Towards a new paradigm for securing wireless sensor networks", *Proceedings of ACM Workshop on New Security Paradigm*, Ascona, Switzerland, pp.115-121, August 2003.

[13] Wenyuan Xu,Ke Ma,Wade Trappe and Yanyang Zhang, "Jamming sensor networks: Attacks and defense strategies", *IEEE Network*, vol.20, no.3, pp.41-47, June 2006.

[14] A.D.Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, vol.35, no.10, pp.54-62, October 2002.

[15] A.S.Wander, N.Gura, H.Eberle, V.Gupta and S.C.Shantz, "Energy analysis of public key cryptography for wireless sensor networks", *Proceedings of 3rd IEEE International Conference on Pervasive Computing and Communications*, Hawaii, pp.324-328, March 2005.

[16] M.Brown, D Cheung, D.Hankerson , J.L.Hernandez, M.Kirkup and A.Menezes, "PGP in constrained wireless devices", *Proceedings of 9th USENIX Security Symposium*, Denver, Colorado, pp.19, August 2000.

[17] D.W.Carman, P.S.Kruus and B.J.Matt, "Constraints and approaches for distributed sensor network security", NAI Labs, *Technical Report 00-010*, 2000.

[18] P.Ganesan, R.Venugopalan, P.Peddabachagari, A.Dean, F.Muller and M.Sichitiu, "Analysing and modeling encryption overhead for sensor network nodes", *Proceedings of 2nd ACM International Conference on Wireless Sensor Networks and Applications*, San Diego, USA, pp.151-159, September 2003.

[19] S.Slijepcevic, M.Potkonjak, V.Tsiatsis, S.Zimbeck and M.B.Srivastava, "On communication security in wireless adhoc sensor network", *Proceedings of 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Pittsburgh, USA, pp.139-144, June 2002.

[20] M.Chen, W.Chen, W.Cui, W.Wen and A.Woo, "Security and deployment issues in sensor network", *Report, Department of Electrical Engineering and Computer Science*, University of California, California, December 2000.

[21] S.A.Camptepe and B.Yener, "Key distribution mechanisms for wireless sensor networks: A survey", *Technical Report, TR-05-07, Department of Computer Science*, Rensselaer Polytechnic Institute, Newyork, USA, March 2005.

[22] D.Liu and P.Neng, "*Security for wireless sensor networks*", Springer, New York, 2007.

[23] J.Lopez and J.Zhou, "W*ireless sensor network security*", IOS Press, Washington, 2008.

[24] Devesh Jinwala, Dhiren Patel and K S Dasgupta, "A survey of the security issues in wireless sensor networks", *ADIT Journal of Engineering*, vol.3, no.1, pp.17-29, December 2006.

[25] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and J.D.Tygar, "SPINS: Security protocols for sensor networks", *Proceedings of ACM Seventh Annual International Conference on Mobile Computing and Networking*, Rome, Italy, pp.189-199, July 2001.

[26] C.Karlof, N.Sastry and D.Wagner, "Tinysec: A link-layer security architecture for wireless sensor networks", *Proceedings of 2nd International Conference on Embedded Networked Sensor systems*, Baltimore, USA, pp.162-175, November 2004.

[27] Yiang Xiao, "*Security in sensor networks*", Auerbach Publications, New York, 2007.

[28] S.A.Camtepe and B.Yener, "Combinational design of key distribution mechanisms for wireless sensor networks", *IEEE/ACM Transactions on Networking*, vol.15, no.2, pp.346-358, April 2007.

[29] J .Kohi and B.Neuman, "The Keberos network authentication service", *IETF RFC 1510*, 1993.

[30] Neuman and Tso, "Kerberos: An authentication service for computer networks", *IEEE Communication Magazine*, vol.32, no.9, pp.33-38, September 1994.

[31] G.Ateniese,M.Steiner and G.Tsudik, "New multi party authentication services and key agreement protocols", *IEEE Journal on Selected Areas in Communication*, vol.18, no.4, pp.628-639, April 2000.

[32] I.Ingemarsson, D.T.Tang and C.K.Wong, "A conference key distribution system", *IEEE Transactions on Information Theory*, vol.28, no.5, pp.714-720, September 1982.

[33] K.Becker and U.Wille, "Communication complexity of group key distribution", *Proceedings of 5th ACM Conference on Computer and Communication Security*, California, USA, pp.1-6, November 1998.

[34] M.Burmester and Y.Desmedt, "A secure and efficient conference key distribution system", *Proceedings of EUROCRYPT'94 Workshop on Theory and Application of Cryptographic Techniques*, Perugia, Italy, pp.275-286, May 1994.

[35] M.S.Hwang, "Dynamic participation in a secure conference scheme for mobile communication", *IEEE Transactions on Vehicular Technology*, vol.48, no.5, pp.1469-1474, September 1999.

[36] X.Yi, C.K.Siew, C.H.Tan and Y.Ye, "A secure conference scheme for mobile communication", *IEEE Transactions on Wireless Communication*, vol.2, no.6, pp.1168-1177, November 2003.

[37] R.Blom, "An optimal class of symmetric key generation system", *Proceedings of EUROCRYPT'84 Workshop on Theory and Application of Cryptographic Techniques*, Paris, France, pp.335-338, April 1984.

[38] C.Blundo, A.De Santis, A.Herzberg, S.Kutten, U.Vaccaro and M.Yung, "Perfectly secure key distribution for dynamic conferences", *Proceedings of 12th Annual International Cryptology Conference on Advances in Cryptology*, California, USA, pp.471-486, August 1992.

[39] L.Eschenauer and V.Gligor, "A key management scheme for distributed sensor networks", *Proceedings of 9th ACM Conference on Computer and Communication Security*, Washington, USA, pp.41-47, November 2002.

[40] H.Chan, A.Perrig and D.Song, "Random key redistribution schemes for sensor networks", *Proceedings of IEEE Symposium on Security and Privacy*, California, USA, pp.197-213, May 2003.

[41] R.Pietro, L.Mancini and A.Mei, "Random key-assignment for secure wireless sensor networks", *Proceedings of 1st ACM Workshop on Security of Adhoc and Sensor Networks*, Virginia, USA, pp.62-71, October 2003.

[42] D.Liu and P.Ning, "Establishing pairwise keys in distributed sensor networks", *Proceedings of 10th ACM Conference on Computer and Communication Security*, Washington, USA, pp.52-61, October 2003.

[43] S.Zhu, S.Setia and S.Jajodia, "LEAP: Efficient security mechanism for large-scale distributed sensor networks", *Proceedings of 10th ACM Conference on Computer and Communication Security*, Washington, USA, pp.62-72, October 2003.

[44] Jing Deng, Richard Han and Shivakant Mishra , "INSENS: Intrusion-tolerant routing for wireless sensor networks", *Journal of Computer Communications*, vol.29, no.2, pp.216-230, January 2006.

[45] A.D.Wood, L.Fang, J.A.Stankovic and AT.He, "SIGF: A family of configurable, secure routing protocols for wireless sensor networks", *Proceedings of ACM Workshop on Security of Adhoc and Sensor Networks*, Virginia, USA, pp.32-48, October 2006.

[46] Hao Yang, Starsky H.Y.Wong, Songwu Lu and Lixia Zhang, "Secure diffusion for wireless sensor networks", *Proceedings of 3rd International Conference on Broadband Communications, Networks and Systems*, California, USA, pp.1-10, October 2006.

[47] C.Intanagonwiwat, R.Govindan and D.Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", *Proceedings of 6th Annual International Conference on Mobile Computing and Networks*, MA, USA, pp.56-67, August 2000.

[48] Suk-Bok Lee and Yoon-Hwa Choi, "A secure alternate path routing in sensor networks, *Journal of Computer Communication*, vol.30, no.1, pp.153-165, December 2006.

[49] W.Du, J.Deng ,Y.S.Han and P.K.Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", *Proceedings of 10th ACM Conference on Computer and Communication Security*, Washington, USA, pp.42-51,October 2003.

[50] W.Du, J.Deng ,Y.Han ,S.S.Chen and P.K.Varshney, "A key management scheme for wireless sensor networks using deployment knowledge", *Proceedings of 23rd Annual Joint Conference of IEEE Computer and Communication Societies* , Hong Kong , pp.586-597, March 2004.

[51] R.D.Pietro, L.M.Mancini, Y.W.Law, S.Etalle and P.Havinga, "LKHW: A direct diffusion based secure multicast scheme for wireless sensor networks", *Proceedings of 32nd International Conference on Parallel Processing Workshops*, Kaohsiung, Taiwan, pp.397-412, October 2003.

[52] M.Eltoweissy, H.Heydari, L.Morales and H.Sudborough, "Combinatorial optimization of group key management", *Journal of Network and Systems Management*, vol. 12, no.1, pp.33-50, March 2004.

[53] M.Chorzempa, J.Park and M.Eltoweissy, "SECK: Survivable and efficient clustered keying for wireless sensor networks", *Proceedings of IEEE Workshop on Information Assurance in Wireless Sensor Networks*, Phoenix, AZ, pp.455-468, April 2005.

[54] Y.Zhang, W.Liu, W.Lou and Y.Fang, "Securing sensor networks with location based keys", *Proceedings of IEEE Conference on Wireless communication and Networking*, Florida, USA, pp.1909-1914, March 2005.

[55] S.Marti, T.Giulli, K.Lai and M.Baker, "Mitigating, routing misbehaviour in mobile adhoc networks", *Proceedings of ACM/IEEE 6th Annual International Conference on Mobile Computing and Networking*, Boston, USA, pp.255-265, August 2000.

[56] S.Buchegger and J.Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in distributed adhoc networks", *Proceedings of the 3rd ACM International Symposium on Mobile Adhoc Networking and Computing*, Lausanne, Switzerland , pp.226-236, June 2002.

[57] P.Michiardi and R.Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile adhoc networks", "*Proceedings of IFIP TC6/TC11 6th Joint Working Conference on Communication and Multimedia Security*, Slovenia, Kluwer, vol.228, pp.107-121, September 2002.

[58] R.Karvets, S.Yi and P.Naldurg, "Security aware adhoc routing protocol for wireless networks", *Proceedings of ACM International Symposium on Mobile Adhoc Networking and Computing,* California, USA, pp.299-302, October 2001.

[59] K.Sanzgiri, B.Dahill, B.N Levine, C.Shields and E.M. Belding Royer, "A secure routing protocol for adhoc networks", *Proceedings of 10th IEEE International Conference on Network Protocol*, Paris, France, pp.78-87, November 2002.

[60] S.Carter and A.Yasinac, "Secure position aided adhoc routing", *Proceedings of the IASTED Conference on Communications and Computer Networks,* Cambridge, MA, USA, pp.329-324, November 2002.

[61] Yih-Chun Hu, D.B.Johnson and A.Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless adhoc networks", *Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications*, NewYork, USA, pp.3-13, June 2002.

[62] C.E.Perkins and P.Bhagwat, "Highly dynamic destination sequenced distance vector routing for mobile computers", *Proceedings of SIGCOMM Conference on Communications Architecture, Protocols and Applications,* London, UK, pp.234-244, August1994.

[63] Yih-Chun Hu, A.Perrig, D.B.Johnson, "ARIADNE: A secure on demand routing protocol for adhoc networks", *Proceedings of ACM Eighth Annual International Conference on Mobile computing and Networking*, Atlanta, USA, pp.12-23, September 2002.

[64] P.Papadimitratos and Z.J.Haas, "Secure routing for mobile adhoc networks", *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonia, Texas, pp.27-31, January 2002.

[65] Yih-Chun Hu, A.Perig and D.B.Johnson, "Packet Leashes: A defense against wormhole attacks in wireless networks", *Proceedings of 22nd Annual Joint Conference of IEEE Computer and Communications*, San Francisco, USA, pp.976-1986, April 2003.

[66] Jeffery Undercoffer, S.Avancha, A.Joshi and J.Pinkston, "Security for sensor networks", *Proceedings of CADIP Research Symposium*, Baltimore, USA, 2002.

[67] Taejoon Park and Kang G.Shin, "LiSP: A lightweight security protocol for wireless sensor networks", *ACM Transactions on Embedded Computing Systems*, vol.3, no.3, pp.634-660, August 2004.

[68] Riaz ahamed Shaikh, Sungyoung Lee, Mohammad A.U. Khan and Young Jae Song, "LSec: Lightweight security protocol for distributed wireless sensor network", *Proceedings of IFIP TC6 11th International Conference on Personal Wireless Communications*, Albacete, Spain, pp.367-377, September 2006.

[69] Lazos and R.Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks", *Proceedings of 3rd ACM workshop on Wireless Security*, Philadelphia, USA, pp. 21-30, October 2004.

[70] S.Capkun and J.P.Hubaux, "Secure positioning of wireless devices with application to sensor networks", *Proceedings of 24th Annual Joint Conference of IEEE Computer and Communication Societies*, Florida, USA, vol.4, pp.1917-1928, March 2005.

[71] F.Anjum, S.Pandey and P.Agrawal, "Secure localisation in sensor networks using transmission range variation", *Proceedings of IEEE Conference on Mobile Adhoc and Sensor System workshop*, Washington, USA, pp.195-203, November 2005.

[72] Wang Xiao-yun, Yang Li-zhen and Chen Ke-fei, "SLEACH: Secure low energy adaptive clustering hierarchy protocol for wireless sensor networks", *Wuhan University Journal of Natural Science*, vol.10, no.1, pp.127-131, January 2005.

[73] W.R.Heinzelman, A.Chandrakasan and H.Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", *Proceedings of IEEE 33rd Hawaii International Conference on System Sciences*, Hawaii, pp.1-10, January 2000.

[74] Jamil Ibriq and Imad Mahgoub, "A secure hierarchical routing protocol for wireless sensor networks", *Proceedings of IEEE International Conference on Communication Systems*, Singapore, pp.1-6, October 2006.

[75] Rajendra Prasad Mahapatra and Mohit Katyal, "Taxonomy of routing security for adhoc network", *International Journal of Computer Theory and engineering*, vol.2, no.2, pp.303-307, April 2010.

[76] Karan Singh,Rama Shankar Yadav and Ran Vijay, "A review paper on adhoc network security", *International Journal of Computer Science and Security*, vol.1, no.1, pp.52-69, June 2007.

[77] Tanveer Ahamed Zia, "A security framework for wireless sensor networks", *Ph.D. Thesis Report, School of Information Technologies*, University of Sydney, February 2008.

[78] Kalpana Sharma, M.K.Ghose and Kuldeep, "Complete security framework for wireless sensor network", *International Journal of Computer Science and Information Security*, vol.3, no.1, pp.196-202, July 2009.

[79] D.Denning, "A new paradigm for trusted systems", *Proceedings of ACM Workshop on New Security Paradigms*, Novascotia, Canada, pp.36-41, September 1993.

[80] Pirzada and C.McDonald, "Establishing trust in pure adhoc networks", *Proceedings of the 27th Australasian Computer Science Conference*, Dunedin, New Zealand, vol.26, no.1, pp.47-54, January 2004.

[81] Asad Amir Pirzada,Chris McDonald and Amitava Datta, "Performance comparison of trust-based reactive routing protocols", *IEEE Transactions on Mobile Computing*, vol.5, no.6, pp.695-710, June 2006.

[82] D.B.Johnson, D.A. Maltz and Y.Hu, "The dynamic source routing protocol for mobile adhoc networks", *IETF MANET, Internet Draft*, 2003.

[83] Zhongwei Zhang and Hong Zhou, "Empirical examination of mobile adhoc network routing protocols on wireless sensor networks", *International Journal of Computer Networks and Communications*, vol.1, no.1, pp.75-87, April 2009.

[84] Asar Ali and Zeeshan Akbar, "Evaluation of AODV and DSR routing protocols of wireless sensor networks for monitoring applications, *Thesis Report, Department of Electrical Engineering with Telecommunication*, Blekinge Institute of Technology, Sweden, October 2009.

[85] Asad Amir Pirzada and Chris McDonald, "Circumventing sinkholes and wormholes in wireless sensor networks", *Proceedings of 2nd IEEE International Workshop on Wireless Adhoc Networking*, London, UK, pp.132-150, May 2005.

[86] Asad Amir Pirzada , Amitava Datta and Chris McDonald, " Trust-based routing for adhoc wireless networks", *Proceedings of 12th IEEE International Conference on Networks* , vol.1, pp.326-330, November 2004.

[87] Georgy Sklyarenko, "AODV routing protocol", *Seminar Technische Informatik*, Institut fur Informatik, Freie Universitat, Berlin, Germany, July 2006.

[88] C.Perkins, E,Royer and S.Das , "Adhoc on-demand distance vector routing", *RFC-3651, IETF Network Working Group*, July 2003.

[89] Zhongwei Zhang , Hong Zhou and Jason Gao, "Scrutinizing performance of adhoc routing protocols on wireless sensor networks", *Proceeding of IEEE First Asian Conference on Intelligent Information and Data base Systems*, Dong Hoi, pp.459-464, April 2009.

[90] Kamal Deep Meka, Mohit Virendra and Shambhu Upadhyaya, "Trust based routing decisions in mobile adhoc networks", *Proceedings of 2nd Workshop on Secure Knowledge Management*, Brooklyn, New York, September 2006.

[91] M.Virendra, M.Jadliwala, M.Chandrasekar and S.Upadhyaya, "Quantifying trust in adhoc networks", *Proceedings of IEEE International Conference on Integration of Knowledge Intensive Multi Agent System*, Waltham, MA, pp.65-71, April 2005.

[92] Brad Karp and H.T.Kung, "GPSR: Greedy perimeter stateless routing for wireless sensor networks", *Proceedings of 6th International Conference on Mobile Computing and Networking*, Boston, pp.243-254, August 2000.

[93] Asad Amir Pirzada and Chris McDonald, "Trusted greedy perimeter stateless routing", *Proceedings of 15th IEEE International Conference on Networks*, Adelaide, Australia, pp.206-211, November 2007.

[94] Razia Haider,Muhammad Younus Javed and Naveed S.Khattak, “Design and implementation of energy aware algorithm using greedy routing for sensor networks”, *International Journal of Security and its Applications,* vol.2, no.2, pp.71-86, April 2008.

[95] Sachin Sharma, H.M.Gupta and S.Dharmaraja, “EAGR: Energy aware greedy routing scheme for wireless Adhoc networks”, *International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, David Hume Building and William Robertson Building, Edinburgh, UK, pp.122-128, June 2008.

[96] Natarajan Meghanathan, “An energy-aware greedy perimeter stateless routing protocol for mobile Adhoc networks”, *International Journal of Computer Applications*, vol.9, no.6, pp.30-35, November 2010.

[97] I.Downard, “Simulating sensor networks in ns-2,” *NRL Formal Report 5522-04-10*, Naval Research Laboratory, Washington, May 2004.

# LIST OF PUBLICATIONS

## INTERNATIONAL JOURNALS

1. "Performance evaluation of homogeneous and heterogeneous sensor networks", *MASAUM Journal of Computing*, vol.1, no.2, pp.377-381, October 2009, ISSN: 2076-0833.

2. "Secured reactive routing protocol for mobile nodes in sensor networks", *WSEAS Transactions on Communications*, vol.9, no.3, pp.216-224, March 2010, ISSN: 1109-2742.

3. "Secured greedy perimeter stateless routing for wireless sensor networks', *International Journal of Adhoc Sensor and Ubiquitous Computing*, vol.1, no.2, pp.9-20, June 2010, ISSN: 0976-1764.

4. "Performance analysis of trust based AODV for wireless sensor networks", *International Journal of Computer Applications*, vol.4, no.12, pp.6-13, August 2010, ISSN: 0975-8887.

## INTERNATIONAL CONFERENCES

1. "Implementation of security mechanism in wireless sensor networks", *Proceedings of International Conference on RF and Signal Processing System*, VijayWada, pp. 243-247, February 2008.

2. "Performance evaluation of heterogeneous sensor networks", *Proceedings of International conference on Future Computer and Communication*, Kuala Lumpur, Malaysia, pp.264-267, April 2009**,** ISBN-13:978-0-7695-3591-3.

3. "Secured dynamic routing protocol for mobile sensor networks", *Proceedings of WSEAS International conferences on Networks, VLSI and Signal Processing*, Cambridge, U.K., pp.19-23, February 2010, ISBN: 978-90-474-162-5.

# VITAE

**P.SAMUNDISWARY** was born in Pondicherry, India in 1975. She received B.Tech. and M.Tech. degree in Electronics and Communication Engineering from Pondicherry Engineering College, Pondicherry University, Pondicherry in 1997 and 2003. She has ten years of teaching experience. She has worked as Assistant Professor in the Department of Electronics and Communication Engineering at Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, Pondicherry, India. Presently, she is working as Assistant Professor in the Department of Electronics Engineering, Pondicherry University. She is a part time Research Scholar in the Department of Electronics and Communication Engineering, Pondicherry Engineering College, Pondicherry, India. She has published four papers in International Journals and three papers in International Conferences. Her area of interest includes Computer Networks, Wireless Networks and Wireless Communication.