INVESTIGATIONS ON ENERGY AWARE INTRUSION DETECTION MECHANISM FOR ZIGBEE WIRELESS SENSOR NETWORKS

A THESIS

submitted by

G. JEGAN

[Reg. No. : 13166006]

in fulfilment for the award of the degree

of

DOCTOR OF PHILOSOPHY

in

ELECTRONICS ENGINEERING

DEPARTMENT OF ELECTRONICS ENGINEERING

SCHOOL OF ENGINEERING AND TECHNOLOGY

PONDICHERRY UNIVERSITY

PUDUCHERRY-605 014, INDIA

MAY 2017

Dr. P. Samundiswary
Assistant Professor
Department of Electronics Engineering
School of Engineering and Technology
Pondicherry University
Puducherry, India

CERTIFICATE

This is to certify that this thesis titled **"INVESTIGATIONS ON ENERGY AWARE INTRUSION DETECTION MECHANISM FOR ZIGBEE WIRELESS SENSOR NETWORKS"** is the bonafide work of **Mr. G. JEGAN [Reg.No:13166006]** who carried out the research work under my supervision. Further, certified that to the best of my knowledge, the work reported herein does not form part of any other thesis or any other degree or award was conferred on an earlier occasion for this or any other candidate.

Place: Puducherry
Date:

Dr. P. SAMUNDISWARY
(Research Supervisor)

ABSTRACT

Wireless Sensor Network (WSN) is a spatially distributed autonomous sensor network consisting of tiny nodes with sensing, computation and wireless communications capabilities. WSNs have drawn a lot of attention due to their broad applications including environmental, healthcare and agriculture monitoring, military surveillance, disaster management and many more. ZigBee, an IEEE 802.15.4 based wireless sensor networks have been the promising technology of facilitating large-scale and real-time data processing in complex environments. IEEE 802.15.4 is the communication protocol proposed for Low Rate Wireless Personal Area Network (LR-WPAN) /Zigbee based sensor networks. Network security with optimum energy consumption is essential to the success of zigbee based WSN applications, especially for the mission-critical applications working in unattended and even hostile environments. However, providing security with optimum energy to ZigBee WSN is a challenging task due to various constraints of Zigbee networks such as limited resource constraints, deployment of nodes in harsh environment and wireless medium. This motivates the research on security mechanism for zigbee based WSN.

This present research work is mainly focused on detecting and preventing security attacks in network layer and Media Access Control (MAC) layer of ZigBee based WSN. Due to increased security threats in different layers of ZigBee based WSN, developing a security mechanism for defending all types of attacks is one of the important challenges in ZigBee based WSN networks. Even though, many traditional ZigBee based WSN security mechanism such as standard encryption algorithms or other cryptographic techniques and secured routing protocols have in built security features, these mechanisms require more memory, energy and computational overhead which are not suitable for resource constraint networks like zigbee WSN. They are also still vulnerable to certain security attacks like Distributed Denial-of-service (DDoS) in the data link layer, hole attacks (wormhole, sinkhole black hole), hello flooding and Sybil types in the network layer. These attacks can easily degrade the performance of network. Hence, in this research work, based on the extensive literature survey, it is intended to focus on designing an Intrusion Detection System (IDS) with energy prediction to identify and prevent the network from DDOS (Energy Exhaustion) attack and also energy aware IDS with different routing

protocols such as AODV, STR and OSTR to identify and prevent the network from wormhole attack in order to provide better security and optimal energy to the ZigBee based wireless sensor network.

The entire research work is divided into four modules. All the four research modules are investigated through NS-2 simulation. In the first module, Energy Efficient Intrusion Detection System with Energy Prediction (EE-IDSEP) is developed to detect DDoS (Energy Exhaustion) attack and the performance parameters such as Packet Delivery Ratio (PDR), energy consumption and end-to-end delay are analyzed through simulation. In second module, the Energy Efficient Intrusion Detection System (EE- IDS) with Adhoc On demand Distance Vector (AODV) protocol is proposed for Zigbee based Wireless Sensor Networks to detect wormhole attacks. Further, the performance metrics such as PDR, end-to-end Delay, and energy consumption are evaluated through simulation. To enhance the performance of network still further and to detect wormhole attack, EE-IDS with Shortcut Tree Routing (STR) is developed which is considered as third module. In addition, the performance of the ZigBee WSN by using EE-IDS-STR such as PDR, end-to-end delay, and energy consumption are examined through simulation. In the fourth module, EE-IDS with Opportunistic Shortcut Tree Routing (OSTR) is developed to detect wormhole attacks. Moreover, the above-mentioned performance metrics are studied through simulation by considering EE-IDS-OSTR. Finally, the proposed EE-IDSEP and EE-IDS are also evaluated by examining the various significant parameters of IDS such as Detection Rate (DR), False Positive Rate (FPR) and detection time.

It is observed from the simulation results that the proposed system EE-IDSEP with respect to DDoS attacks outperforms the existing system EE-TS in terms of performance metrics such as PDR, average end-to-end delay, energy consumption, detection rate, FPR and detection time. Further, the proposed EE-IDS for detection of wormhole attack achieves overall better performance in terms of above mentioned performance metrics than that of existing EE-TSW.

ACKNOWLEDGEMENT

First, I would like to express my sincere gratitude to my supervising guide, **Dr. P. SAMUNDISWARY**, Assistant Professor, Department of Electronics Engineering, Pondicherry Central University for her guidance, encouragement and the timely care that she rendered to me during my research period. Her tremendous technical and mental support has been a steady state of inspiration to me. I shall forever cherish the exposure and facilities that she offered during period of my research under her guidance.

I express my profound gratitude and obligation to my doctoral committee members, **Dr. G. FLORENCE SUDHA**, Professor, Department of Electronics and Communication Engineering, Pondicherry Engineering College, Puducherry and **Dr. S. RAVI**, Assistant Professor, Department of Computer Science, Pondicherry Central University for their well time care and valuable suggestion throughout my research period.

I express my sincere gratitude to **Dr. R. NAKKEERAN,** Associate Professor and Head, Department of Electronics Engineering, Pondicherry University for the kind hearted support and care during my research period.

I am grateful to **Dr. P. DHNAVANTHAN**, Professor and Dean (i/c), School of Engineering and Technology, Pondicherry University and Professor **Dr. R. SUBRAMANIAN** , Former Dean , School of Engineering and Technology for their whole hearted support and inspiration during my research period.

I express my humble gratitude to **Dr. ANISHA BASHEERKHAN**, Vice Chancellor (officiating), Pondicherry Central University for providing facilities to complete the research work at the earliest. I thank all the teaching and non-teaching staffs of the Department of Electronics Engineering, Pondicherry University for their friendly support and care during my research period.

I would also like to thank all my dear co-researchers, **Mr. R. Vassoudevan, Mrs. Rekha Kamban, Ms. M. Sivasindhu, Mr. A. Nallathambi, Mr. M. Raj Kumar Naik and Mr. K. V. Gowreesrinivas** for their kind support, motivation and suggestions throughout my research work. Finally, I thank the almighty God for blessing and helped me to complete this research work successfully.

JEGAN.G

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	Adhoc On demand Distance Vector
BEARP	Routing protocol Based on Encryption and Authentication
DDoS	Distributed Denial of Service
DR	Detection Rate
DTN	Delay-Tolerant Networks
EE-IDS	Energy Efficient Intrusion Detection System
EE-IDSEP	Energy Efficient Intrusion Detection System with Energy Prediction
EE-TS	Energy Efficient Trust System
EE-TSW	Energy Efficient Trust System for Wormhole attack
FPR	False Positive Rate
GTS	Guaranteed Time Slots
HMM	Hidden Markov Model
IDS	Intrusion Detection System
MAC	Medium Access Contol
OSTR	Opportunistic Shortcut Tree Routing
PDR	Packet Delivery Ratio
QD	Queue Delay
QoS	Quality of Service
RERR	Route ERRor
RREP	Route REPly
RREQ	Route REQuest
RPSS	Routing Path Selection System
SCMRP	Secure Cluster based Multipath Routing Protocol
SERP	Secure Energy Efficient Routing Protocol
SC-LEACH	SeCure Low-Energy Adaptive Clustering Hierarchy
STR	Shortcut Tree Routing
SIGF	Secure Implicit Ge- ographic Forwarding
TIT	Topology Information Table
WSN	Wireless Sensor Network

CHAPTER-1

INTRODUCTION

1.1 GENERAL

The rapid development of Wireless Sensor Network (WSN) is the most recent pattern of Moore's law towards the scaling down and ubiquity of computing devices. Generally, WSN is a wireless network consists of spatially disbursed autonomous tiny devices called sensor nodes used for several true applications such as ecological monitoring, healthcare monitoring, habitat monitoring, military surveillance, home security networks, earth science and exploration and so on. However, the limitations of these nodes are less energy, limited memory and computational ability. These limitations provide massive research challenges such as energy awareness, routing, architecture design and security. As these networks are deployed in hostile and unattended environment and due to its broadcast nature of communication, WSN are vulnerable to several types of security attacks such as physical tampering, node capture, eavesdropping, routing and Distributed Denial of Service (DDoS) attacks. Even though the existing security mechanisms such as authentication, cryptography or key management techniques and secure routing protocol defend the security attacks, they are not feasible for resource-constrained networks such as WSN and ZigBee based WSN due to requirement of more memory and high overhead. The primary focus of this thesis is to provide security to the resource constrained wireless networks such as ZigBee WSN in the presence of security attacks such as wormhole and DDoS attack and prevent the network from that attacks.

1.2. WIRELESS SENSOR NETWORK

WSN [1] comprises tiny nodes with sensing, computation and wireless communications capabilities combined with each other. WSN consists of fundamental modules such as, (i) Wireless Sensor Node (ii) Base Station / Sink Node and (iii) Wireless Link as shown in figure-1.1. The communication between the nodes and the nodes to the sink or base station is made by using radio transceiver with built-in antenna or connection with an external antenna. Then, it is communicated with the end user by using either wired or wireless link.

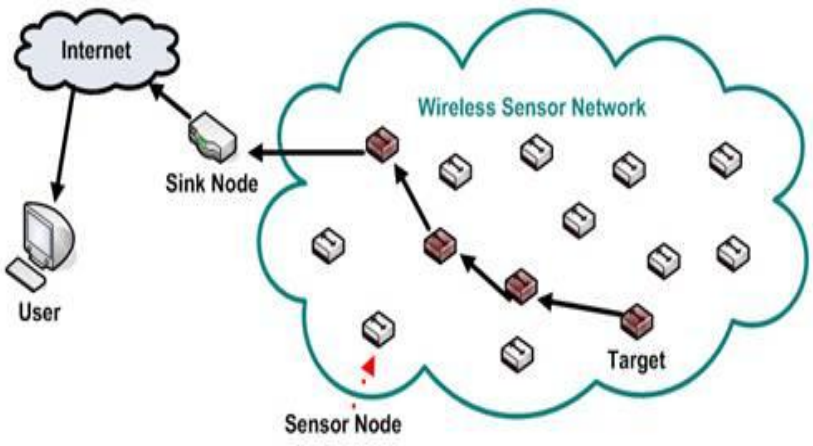


Figure 1.1 Typical WSN Architecture [1]

Typically, the architecture of the WSN shown in figure 1.1 is influenced by various factors such as production cost, fault tolerance, memory constraints, energy consumption, operating environment, transmission media and security. These constraints have to be considered while designing a WSN system to make it feasible for various applications [2] including automation, entertainment, monitoring, security and asset tracking. Nowadays, WSN with ZigBee technology have been used in many applications mentioned above including Internet of Things (IoT) due to its attracted features such as low energy consumption, operated in 2.4 GHz frequency band and low cost.

1.2.1 Zigbee Wireless Sensor Network

ZigBee [3] is an attempt to fabricate a broadly useful WSN on top of IEEE 802.15.4, including security, multi hop routing and Application Programming Interface (API). It is otherwise known as Low Rate Wireless Personal Area Network (LR-WPAN). ZigBee WSN is one of the wireless standard technologies intended to address the wireless sensor and control networks with distinctive requirements of low power consumption and low cost. The sensor device utilized in this network has maximum operating frequency of 2.4 GHz with 250 Kbps data rate; it also supports other frequency bands such as 868 and 928 MHz with full duplex wireless data transmission.

ZigBee standard builds up the structure for the network and application layers in view of the PHY and MAC layers defined by IEEE 802.15.4 standard [4-5]. It defines the hierarchal

structure for the functioning of sensor nodes such as coordinators, routers, and end devices as shown in figure 1.2. Among the three different functioning devices, the ZigBee coordinator is the heart of the network and responsible for the network formation through network discovery and controlling all other devices in the network. Ordinarily it also acts as a trust centre of the Zigbee wireless sensor network. A trust centre is an application operated by a ZigBee coordinator, which ensures the authentication of the devices attached to the network. Another device called ZigBee router, which is responsible for routing function and pass on the traffic through the network. Routers can also be configured as coordinators if needed. A third device in the ZigBee hierarchical structure is ZigBee end device. It is a normal sensor node having simple function of sending the data to router/ coordinator or receiving the data from router or coordinator. It cannot route packets on its own, rather it depends on its parent to deal with all the routing. The function of end device is made considerably simpler than coordinator and router to reduce the power consumption so as to enhance the lifetime of the network.

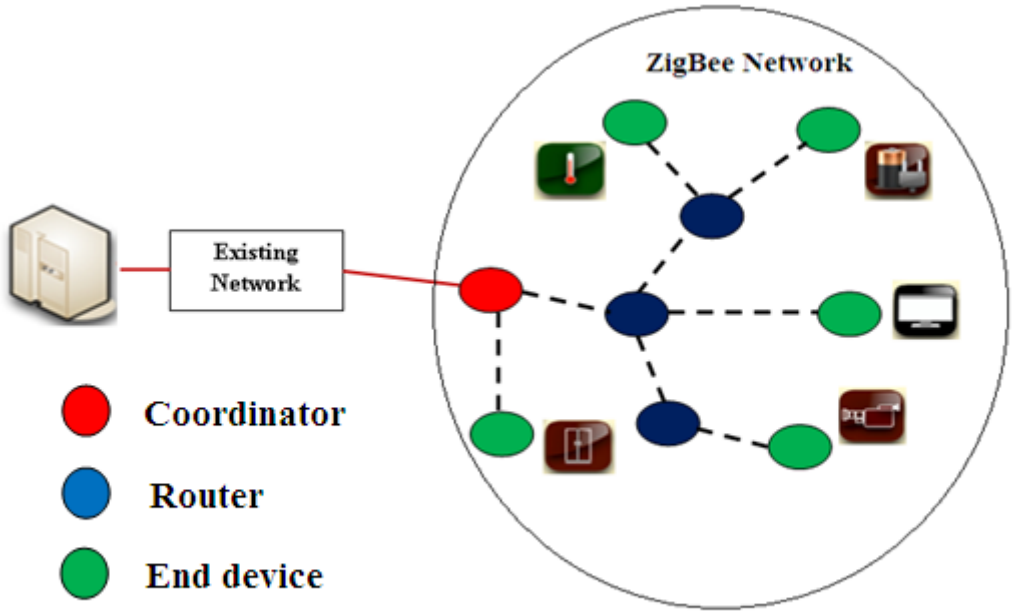


Figure 1.2 Typical ZigBee WSN Architecture

ZigBee WSN plays a vital role in operation and maintenance of environmental monitoring, habitat exploration of animals, remote patient monitoring, military battlefield

surveillance, forest fire and flood detection, power grid and controlling home appliances. However, providing security to ZigBee WSN is a challenging task due to wireless medium and massive deployment of nodes in physically unsecured environment. The following section deals with the security aspects of Zigbee WSN.

1.3 SECURITY IN ZIGBEE WSN

Even though, the standard encryption algorithms [6-7] or other cryptographic techniques [8-10] and secured routing mechanism are developed for ZigBee sensor networks, they are concentrating only for data security not for node security. ZigBee network is still highly vulnerable to energy exhaustion attacks, replay attacks, network discovery attacks and routing attacks. Due to the memory and energy constraints of sensor nodes in a ZigBee WSN, various security solutions developed for IP networks are not suitable for ZigBee WSN.

Security Goals in ZigBee WSN

The security objectives of a secured framework for a ZigBee WSN don't vary much from the security objectives of other secured wireless networks. A more explicit description of these objectives are explained underneath.

Confidentiality

The objective of confidentiality is to guarantee that an adversary cannot read the information being exchanged. As a wireless sensor network might handle important information, for example, military or medical information, it is imperative that the confidentiality is required to protect the network from an adversary node. Generally, cryptographic approaches are utilized to ensure secrecy of the information.

Message Authenticity

The objective of the message authenticity is to guarantee that the source and integrity of the information is conceivable to follow. Due to wireless communication, message injection can be done easily while transmission of messages, which causes communication instability or even take over the control of the network. Authenticity is generally ensured by utilizing codes such as a Message Authentication Code (MAC).

Message Integrity

The aim of integrity shield is to guarantee that the message being exchanged has not been altered through malevolence during the transmission of message from source node to destination.

This put an end to an adversary from changing a validated message. Typically MAC is used to provide integrity.

Freshness

The aim of freshness is to guarantee that the message being transferred is recent one and no adversary node has replayed old messages. It is used for defending against replay attacks, where an adversary catches a packet and later resends it with exact validity and integrity codes. Generally, counters are used to ensure the data freshness.

Robustness

The aim of robustness is to guarantee that errors are handled by the system properly even the adversary disturbs the system. Typically robustness in WSN is introduced by designing the protocols with consideration of strategies such as key distribution, routing with guaranteed delivery and activity scheduling and coverage problems.

1.3.1 Security attacks in ZigBee WSN

Generally, security attacks [11] make the network system not to achieve the security goals of the wireless sensor networks. If the security system fails, they expose vulnerabilities. Some of the attacks faced by ZigBee WSN and their defense mechanisms are shown in table 1.1. The security framework for each layer is needed to minimize the impact of these threats.

Table1.1 Security attacks in ZigBee WSN [11]

Network Layer	Attacks	Defending approach
Physical Layer	Jammer	Spread-spectrum techniques, Lower duty cycle, Priority messages.
	Tampering	Tamper proofing, Hiding
Data Link Layer or MAC	Collision	Error correction code
	Energy Exhaustion, Flooding,	Rate Limitation
Network Layer	Spoofing, Steganography attack, wormhole attack	Authentication, Watch dog approach
	Selective forwarding	Probing, Redundancy
	Sink hole	Monitoring, Redundancy, Authentication
Application Layer	Selective message forwarding, Clone attack, Data aggregation distortion and Clock skewing	Unique pair wise keys and cryptographic techniques, encryption and authentication

Physical layer

A denial of service attack in the physical layer disturbs the network performance by jamming the radio communications. Generally, due to the limitation of sensor battery power, a normal sensor device cannot compete with high power transmission of jammer's. The modulation of the signal, spread spectrum techniques and lower duty cycle are the existing methods to offer some protection against these attacks.

MAC layer

Generally, the MAC layer is prone to attacks such as energy exhaustion and flooding. Even though security solution like rate limitation defends against these attacks, still network performance is not achieved at good level due to the lack of security solution in the wireless protocols. Due to MAC layer attacks, the adversary nodes compel the other normal sensor nodes to retransmit messages multiple times and exhaust their energy rapidly by continuously transmitting the message or violating Guaranteed Time Slots (GTS). These attacks can be defended easily by developing the reliable wireless security protocol to strengthen the MAC layer security.

Network layer

Generally, the routing attack is one of the devastating attacks at the network layer, which forms false routing between the source and destination to transmit the data far away through the network to dissipate the power quickly and degrade the global network performance. These attacks can be prevented by security mechanisms such as authentication, monitoring by watchdog nodes and secured routing protocol.

Application layer

Typical attacks involve in the application layer are selective message forwarding, data aggregation distortion and clock skewing. These attacks make the sensor devices forced to do enormous computation or consume huge storage memory. These attacks have a tendency to very explicit for a certain execution. Recently, intruder detection system using watchdog approaches provides better security solution for different attacks of Zigbee Sensor Networks.

1.4. INTRUSION DETECTION SYSTEM

An Intrusion Detection System (IDS) is a system, which is able to identify the adversary nodes, and then rapidly reports the neighbor nodes to carry out counteract. The main challenges

faced by detection system is to improve the performance of IDS metrics in terms of False Positive Rate (FPR) and Detection time, which is difficult to achieve in the case of expansion of networks into large WSN. If the size of the network is bigger, there may be available of huge data transfer, which makes very difficult to predict the networks in real time. The IDS approaches [12-15] achieve better level of performance in terms of security rather than the energy efficiency. But, energy efficiency is an important factor in the WSN particularly for resource constrained ZigBee WSN. Typically, watchdog mechanism is used in the IDS for monitoring the behavioral nature of the nodes in the network to identify the intruders in the network. Moreover, it is the core part of the trust system. However, owing to the high energy consumption of watchdog approach, network lifetime is reduced greatly. Hence, it is required to incorporate optimization technique with the traditional IDS to make the system energy efficient and applicable to .large area of WSN. Generally, IDS's are classified into three major categories. They are:

A. Signature based IDS*:*

It is also known as rule based IDS as they have predefined rules for different security attacks. These IDS can only detect the security attacks whose signatures are present in the databases. It is suitable for large sized WSNs. The limitation of such detection mechanisms is that they cannot detect new or those attack, whose signatures or identities are not present.

B. Anomaly based IDS

*A*nomaly based IDS are intelligent and they do not have a support of predefined rules. It monitors network activities and classifies them as either normal or adversary using threshold values or heuristic approach.. Mostly it uses statistical, probabilistic approaches, traffic analysis or intelligent techniques for detecting the attacks. It is well suitable for small-sized WSN

C. Hybrid IDS

*H*ybrid IDS techniques combines the objective of signature or misuse based approach and anomaly based approach. Even though, it is helpful for finding the known as well as unknown attacks based on monitoring the deviation from the normal behavior of the sensor nodes, it is not well suitable for resource constraint network namely ZigBee WSNs due to more complexity, high energy consumption, huge memory consumption and heavyweight nature.

Among these IDS, security mechanism using signature based IDS is considered for identifying known attacks such as energy exhaustion attacks and hole attacks which are considered in this research work. Although, these types of IDS are used as detecting mechanisms in ad-hoc and WSN networks, it is impracticable to implement directly in ZigBee wireless sensor networks, due to huge variation in their network characteristics such as autonomy, lifetime, node deployment location and self-configurability. It is also a fact that if the network size is larger, the quantity of data being produced is also enormous, which makes real time prediction a difficult task. Thus, ZigBee WSNs require a new and lightweight design of intrusion detection system.

1.5. SCOPE OF THE WORK

In ZigBee WSN, security is a field of incredible significance since ZigBee networks are ready to carry vital information from sensor nodes and additionally they are utilized in controlling various applications. Further, transmission medium of ZigBee WSN networks is wireless in nature. Owing to wireless in nature and deployment of nodes in harsh environment, ZigBee WSN networks is prone to various attacks. However some security approaches such as authentication, key management or cryptography techniques improve the ZigBee based WSNs security, they are consuming more power and memory and also not effective against attacks such as DoS (Denial of Service) and hole attacks [16-17]. In order to improve the security of ZigBee based WSN, the proper security defense scheme is needed for the detection and prevention of DoS and hole attacks.

Packet leashes [18] – geographic and temporal are the popular security solutions for detection of wormhole attack. This solution requires tight clock synchronizations and thus it is hard to achieve with the resource constrained nodes.

SECure tracking Of node encounteRs (SECTOR) protocol [19] is a another security solution to defend against wormhole attacks. In SECTOR, the Mutual Authentication with Distance bounding (MAD) protocol is used. This approach is related to packet leashes at high level, but it does not need location information or clock synchronization. But, it still experiences other limitation such as requirement of special hardware for time measurement with nanosecond precision. Various security mechanisms [21-24] have been developed by researchers to detect and prevent wormhole attacks on wireless adhoc and sensor networks. These security

mechanisms involve graph theoretical approach [21], local monitoring [22] and statistical approach [23-24] to defend against wormhole attacks. Even though these techniques are defending against wormhole attacks, the limitations such as requirement of special hardware, higher energy consumption and lower detection rate makes this system unsuitable for larger area wireless sensor networks.

Subsequently, several secured routing protocols such as SIGF [25], SC-LEACH [26], SERP [27], SCMRP [28], BEARP [29], Directed diffusion [30] and Secure Directed Diffusion [31] have been developed to provide secured routing on wireless sensor networks. The major drawbacks of these secure routing protocols are high-energy consumption, requirement of large memory and bandwidth and higher communication overhead due to exchange of control messages during authentication phase. Hence, it is unsuitable for resource-constrained networks.

In addition, various researchers for defending various attacks in ZigBee wireless sensor networks have developed several key management techniques [32-35]. Since these techniques adopts key pre-distribution scheme (i.e) key information is distributed among all sensor nodes prior to deployment; knowing the set of neighbors deterministically might not be feasible due to the randomness of deployment. Moreover, adding new nodes to the existing sensor network is difficult due to unaware of keys of new nodes by existing nodes. Further more, it does not exhibit network resilience, if the node is compromised node. Hence, the entire network will be compromised.

W. R. Pires et al [36] has presented a solution to identify two kinds of attacks namely wormhole attack and HELLO flood attack in WSN by forming a rule that compares the received signal energy and observed signal energy around the network. Even though, this solution is one of the first solutions in that domain, it is not completely reliable solution to detect the attacks because of change in the signal strength due to some other reasons rather than influence of attacks. This makes this solution impractical to networks that require optimum security and energy consumption.

Several researchers [37-46] have presented DoS and DDoS attacks in MAC layer of IEEE 802.15.4 WSN and also provide the security measures against those attacks for ZigBee WSN. Although, the security approaches provides protection to ZigBee WSN against DoS

attacks, they are not feasible for all kind of applications because of tradeoff between security and energy.

In Fuzzy Based Detection and Prediction System (FBDPS) [47], the DDoS attacks in IEEE 802.15.4 WSN is detected by using fuzzy logic based on the energy consumed by the node. Another trust model called bayesian trust model [48] is presented to detect MAC layer attacks by considering few parameters that are context-dependent along with a flexible ageing factor to enable this trust model as adaptive handling by changing specific network conditions based on various context parameters. This trust model has the limitation of more computational overhead and high energy consumption.

Defeating Energy-Efficient JAMming (DEEJAM) [49] is a novel MAC protocol for detecting the hidden jammers in IEEE 802.15.4 WSN system. In this protocol, four security mechanisms are considered to defeat the effectiveness of the jammer for protecting the data transmission. This protocol efficiently overcomes several complex and dangerous attacks such as, activity jamming, pulse jamming, and scan jamming and interrupts jamming. However, this protocol is used to defend against only jamming attacks not any other attacks.

The traditional decentralized IDS proposed by A.P. da Silva *et al*. [50] is the first and most cited signature or rule based Intrusion detection approach for WSN to identify the various attacks in different network layers. In this system, there are three major phases involved. They are i) Data acquisition phase is meant for promiscuous listening of the data and filtering the vital information by the monitored nodes for the analysis. ii) Rule application phase is for checking the acquired data by applying pre-defined rule; if the data investigation is failed in any of the rules test, a failure is raised and the counter is incremented by one. iii) The IDS phase for producing alarm when failure rate has reached the threshold level. Even though this IDS scheme detects the various attacks in different layers, it is not suitable for resource constrained ZigBee WSN due to high energy consumed by monitor nodes.

Further, there are several IDS [51-62] such as Misuse or signature based IDS, anomoly IDS and hybrid IDS have been presented by various researchers to detect DoS attacks in MAC and network layer for wireless adhoc and sensor networks. Misuse IDS is developed to detect known type of attacks whereas, anomaly IDS for detecting unknown type of attacks. Both known and unknown types of attacks can be detected by using hybrid IDS, but it is unsuitable for resource constrained WSN due to high energy and memory consumption. In case of misuse IDS,

maintaining signatures of attacks to generate data base is a difficult task for WSN because of its limited storage capacity and computational capabilities. Still, in very few literature studies, this method is explored by using watchdog mechanism [63, 64]. Watchdog mechanism uses the abnormal behavior of a node to detect intruders. All watchdog nodes watch the performance of their neighbors and communicate the information about their behavior to the coordinator or trust center for verifying and taking necessary action on the nodes in order to improve the quality of service of the network. However, the energy consumed by watchdog nodes is more, which makes this mechanism incompatible for resource constrained ZigBee WSN.

Yanzhi Ren et al [65] have proposed wormhole detection mechanism for wormhole attacks in Delay-Tolerant Networks (DTN) for military battlefield application. This approach uses the technique of reducing the transmit power of node for short period of time to detect the wormhole attack, this method has been evaluated by considering two mobility models such as random way point and zebranet. Although, it is detected the attack efficiently without use of special hardware, it has achieved only 92% of detection rate.

It is clear that the traditional security mechanisms such as cryptography, key management techniques, secured routing protocol and trust systems have not provided satisfactory security solutions for resource constrained ZigBee WSN to defend against DDoS and hole attacks. Further, those security mechanisms have failed to provide optimum energy consumption to resource constrained WSN. In order to provide enhanced performance of resource constrained ZigBee WSN in terms of network and IDS performance metrics, an attempt has been made in this research work by developing energy efficient intrusion detection system for resource constrained ZigBee WSN in order to provide better security solution against DDoS and wormhole attacks .

1.6. OBJECTIVE

This thesis contributes to the field of enhancing the security in ZigBee wireless sensor network and to improve the performance of the ZigBee WSN by developing Energy Efficient IDS to detect DDoS attack and wormhole attack.

The primary research objectives are:

- ✓ To develop an Energy Efficient Intrusion Detection System with Energy Prediction (EE-IDSEP) for detection of DDoS attack in ZigBee based Wireless Sensor Network and

analyze the performance of the network in terms of Packet Delivery Ratio (PDR), end-to-end delay and energy consumption through simulation.

- ✓ To develop an Energy Efficient Intrusion Detection System (EE-IDS) with Adhoc On demand Distance Vector (AODV) routing protocol for detection of wormhole attack in ZigBee based WSN and evaluate the performance of the network in terms of PDR, end-to-end delay and energy consumption through simulation.
- ✓ To develop an Energy Efficient Intrusion Detection System with Shortcut Tree Routing (STR) protocol for detection of wormhole attack in ZigBee based WSN through simulation and examine the above mentioned performance metrics.
- ✓ To develop an Energy Efficient Intrusion Detection System with Opportunistic Shortcut Tree Routing (OSTR) routing protocol for detection of wormhole attack in ZigBee based WSN through simulation and study the above mentioned performance metrics of the network.
- ✓ Finally, to evaluate the above mentioned four proposed IDS by examining the various significant parameters such as Detection Rate (DR), False Positive Rate (FPR) and detection time through simulation.

The above mentioned proposed schemes and their performance metrics are simulated by using NS-2.

1.7. ORGANIZATION OF THE THESIS

The research work is organized as chapters in this dissertation and the descriptions of all chapters are as follows.

Chapter 1: This chapter describes about the introduction of the ZigBee wireless sensor network and existing Intrusion Detection System (IDS) for ZigBee wireless sensor network. This chapter also discusses about the watchdog mechanism, which is the core part of the intrusion detection system.

Chapter 2: In this chapter, a literature survey of various Intrusion Detection System (IDS) and security mechanisms are dealt for detecting and preventing MAC layer attacks and network layer attacks in WSN.

Chapter 3: This chapter deals with the proposed Energy Efficient Intrusion Detection System with Energy Prediction (EE-IDSEP) for detection of DDoS attacks in the ZigBee wireless sensor

networks and also performance analysis in terms of PDR, end-to-end delay and energy consumption of ZigBee WSN is also discussed with the aid of simulation results

Chapter 4: This chapter describes about the newly developed Energy Efficient Intrusion Detection System (EE-IDS) with Ad-hoc On demand Distance Vector (AODV) protocol for the detection of wormhole attack in the ZigBee WSN and performance metrics of ZigBee WSN such as PDR, end-to-end delay and energy consumption are depicted through simulation results. Further, the various performance parameters of newly developed IDS such as detection rate, False Positive Rate (FPR) and detection time obtained through simulations results are also explained.

Chapter 5: In this chapter, the developed Energy Efficient Intrusion Detection System (EE-IDS) with Shortcut Tree Routing (STR) protocol for the detection of wormhole attack in the ZigBee WSN is dealt. Also, the performance parameters such as PDR, end-to-end delay and energy consumption and further, performance metrics of the newly developed IDS such as detection rate, FPR and detection time are also examined through the simulation results.

Chapter 6: This chapter deals in detail with proposed EE-IDS with Opportunistic Shortcut Tree Routing (OSTR) for detecting wormhole attack and performance analysis of the network in terms of PDR, end-to-end delay and energy consumption is also explained. Further, performance metrics of the IDS such as detection rate, FPR and detection time are also discussed with the aid of simulation results.

Chapter 7: This chapter deals with the conclusion of the research work and scope of the future studies.

CHAPTER-2

REVIEW OF LITERATURE

2.1. GENERAL

The extensive literature collected related to security mechanisms such as encryption , key management schemes, secure routing protocols and Intrusion Detection System (IDS) against various attacks such as routing attacks and DoS attacks exposed by WSN and ZigBee based WSN is critically reviewed and discussed in this chapter. Further, the summary of review of literature is furnished at the end of review to substantiate the scope of present work.

2.2. LITERATURE REVIEW

Hu Y.C, A. Perrig *et al.* [18] have developed a new mechanism called Packet leashes – geographic and temporal, which is the popular security solution for detecting and defending against wormhole attack. However, this mechanism needs exact clock synchronizations, which make the system difficult to realize optimum security with the resource constrained networks.

SECure tracking Of node encounteRs (SECTOR) [19] protocol is an another security solution proposed by Capkun S *et al.* to protect the WSN from wormhole attacks. Mutual Authentication with Distance Bounding (MAD) protocol has been used in SECTOR. Although, this security mechanism is related to packet leashes at high level, it does not need any location information or clock synchronization. However, the requirement of special hardware for time measurement with nanosecond precision makes this security approach applicable to small size WSN

Hu L and Evans D [20] has proposed another protocol namely directional neighbour discovery protocol for preventing wormhole attacks by using directional antennas into a network. Although this protocol defends against wormhole attacks, it imposes all nodes to use directional antenna, which increases the system complexity.

There are few other techniques [21-22] developed by researchers to prevent wormhole attacks on wireless ad hoc networks. These techniques use graph theoretical approach for detecting wormhole attacks. However, these approaches require special hardware and tight clock synchronization among the sensor nodes to prevent the attack in wireless sensor networks.

Some techniques examine the symptoms occurred due to the traffic flow mismatch based on statistic analysis with respect to sensor network traffic. N. Song *et al* [23] examine the fact that the selection of wormhole links for routing are made with abnormally high speed. Since, the data flow made by wormhole link is achieved with high frequency; it can be easily identified by comparing with normal statistics of network. However, it consumes high energy for verifying network statistics.

Buttyan *et al* [24] has developed another statistical approach to defend against the wormhole attack. This approach finds the abnormal increase in number of neighbors and reduces the shortest path length due to wormholes. The wormholes are detected by the base station by using hypothesis testing based on prestatistics of typical networks. However, it is not accurate in detecting the wormhole due to the changing of network statistics by some other factors such as traffic congestion, communication link failure etc., other than influence of wormhole attack.

Secure Implicit Geographic Forwarding (SIGF) is the family of configurable, secure routing protocol for wireless sensor networks developed by Wood et al [25]. It includes three protocols such as SIGF-0, SIGF-1 and SIGF-2. SIGF-0 is the first building block towards secured routing which selects the next-hop non-deterministically and dynamically. SIGF-1 is the extended version of SIGF-0 by keeping and storing reputed information about the neighbors locally. Finally, SIGF-2 provides cryptographic defense against malicious message manipulations and eavesdropping. SIGF-2 defends against attacks such as spoofing, altering or replay attacks, wormhole, hello floods, black holes, selective forwarding, Sybil attacks and DOS attacks. Since, SIGF provides hop-by-hop authentication, which is not adequate to prevent the adversary from diverting the traffic to decrease the network lifetime. In addition, it requires significant storage, communication and computation cost to provide source authentication.

Wang J. *et al* [26] have proposed SeCure Low-Energy Adaptive Clustering Hierarchy (SC-LEACH) routing protocols based on low power cluster-head selection algorithm for WSN. SC- LEACH has adopted pre-shared key pair, thus it has improved the security of the routing effectively than the LEACH. However, by node tampering, pre-shared key can be extracted and made it use for joining into the network by the malicious node in order to steal the confidential data from the network.

Subsequently, Secure Energy Efficient Routing Protocol (SERP) [27] is developed for densely deployed wireless sensor networks. It offers a high level of confidentiality and

authenticity of message that are sending from sensors to the base station. It uses one-way hash chain and pre-stored shared secret keys to guarantee secure message transmission. However, it requires large memory for storing keys to achieve authentication.

Kumar and Jena [28] have developed Secure Cluster based Multipath Routing Protocol (SCMRP) for WSN to provide defense against many attacks such as selective forwarding attack, altering the routing information, sinkhole attack, sybil attack and wormhole attack. This method uses pairwise and unique shared key mechanism. Since it has adopted pairwise and unique shared key, it requires more storage memory; hence it is not suitable for resource constrained network.

Further, an efficient and secure Routing protocol Based on Encryption and Authentication (BEARP) for wireless sensor networks is proposed by J. Zhou [29]. BEARP has three phases: neighbor discovery phase, route discovery and routing maintenance phase. Neighbor discovery phase is initiated by sink node for constructing network topology which is done by periodically broadcasting a packet confidential to all the nodes in the network in order to update their information. Route discovery is a task for finding the routes between source and destination, which is done by the function of three subtasks namely data enquiry, Routing Path Selection System (RPSS) and sending routing information. Finally in route maintenance, the Base Station (BS) works as the server to operate as IDS and to release control message. It ensures the four security features including authentication, confidentiality of routing message, integrity and freshness. It defends against attacks such as node capturing, worm hole, sink hole and selective forwarding. It is evident from the simulation results that BEARP has performed well compared to that of directed diffusion protocol [30] and secured directed diffusion protocol [31] in the presence of malicious or compromised nodes. However, the tradeoff between energy consumption and security makes the system unsuitable for resource constrained networks.

Several key management techniques [32-35] have also proposed for ZigBee wireless sensor networks to defend against the attacks such as wormhole and sink hole attacks in network layer and DoS attacks in MAC layer. It requires excessive storage for each node to store four types of keys. These techniques are not completely resistant to those attacks. Further, the storage cost for the shared key is exponentially increased with group size, which makes it prohibitive in sensor network with low memory capacity.

W. R. Pires *et al* [36] have developed a defense mechanism for detecting attacks such as HELLO flood and wormhole attack in WSN. This approach detects the malicious nodes such as HELLO flood and wormhole attacks by comparing the received signal strength with the expected value and calculated geographical information of the nodes. Since this mechanism uses geographical information from GPS radio system, it requires some degree of cooperation from at least three nodes for finding the approximate region where the attacker is located. This makes this solution impractical to large area of WSN due to the requirement of special GPS radio system.

Wood and Stankovic [37] have given an ample assessment of various DoS attacks and their counter measures and techniques to implement in sensor networks. These attacks are exhibited based on the security vulnerability of the MAC, network and transport layer. An attempt has been made to fortify the requirement for WSN security protocols that are having strong resistant to DoS attacks. Finally, it has been concluded that security contemplations must be included at the design stage of protocol, but not after implementation.

David R. Raymond *et al* [38] have described the denial of service threats and their countermeasures for resource constrained wireless sensor network. Even though, traditional encryption and authentication techniques and other techniques (such as detecting jamming attacks) can defeat many threats in WSN, protecting WSN against denial of sleep attacks is one of the critical problems in widespread deployment of nodes. Hence additional research is needed in low-overhead antireplay protocols for complementing the current authentication techniques to enhance the security on resource constrained WSN.

Various researchers [39-43] have investigated various MAC layer DoS attacks for IEEE 802.15.4 WSN and also have discussed about the counter measures to such type of attacks. However tradeoff between security and energy makes these approaches not to be utilized for small sized WSN.

Subsequently, K. Gill *et al* [44] have proposed a method to protect home based WSN from low level DOS attacks. DOS attack may obstruct the distant access or obtain prohibited access from illicit user. Existing security approaches are generic and not suitable for filtering of unwanted packets.

Eugene *et al* [45] have proposed a security mechanism to identify and prevent legitimate nodes from vampire attack. Vampire attack is one of the brutal attacks which can severely affect

node battery power by draining it quickly. Vampire attack is the improved version of DDOS attack. As this attack utilizes protocol-compliant messages, these are very hard to identify and prevent them from network.

Saman Taghavi Zargar *et al* [46] have investigated the extent of the DDoS flooding attack issues and presented the solution to defend it. Moreover, they have highlighted the requirement for a complete distributed and mutual defense technique. The main goal of this work is to motivate the research society into rising innovative, valuable, efficient and ample prevention, detection and reply mechanisms that deal with the DDoS flooding issues before, during and subsequent to real attack. However, it defends only the particular attack.

C. Balarengadurai *et al* [47] have developed Fuzzy Based Detection and Prediction System (FBDPS) for preventing the DDoS attacks in IEEE 802.15.4 WSN. These approaches have used fuzzy logic based on the energy consumed by the node for defending against the attacks ,which involves more computational process.

Bernardo M. Davidel have presented a security model known as bayesian trust model [48] to detect DoS attacks based on MAC unfairness by using context-dependent and a flexible ageing factor. This model is also suitable for enforcing GTS allocation policies and may serve as a component for more comprehensive Multi-Layer trust model. However, this is not applicable foe large WSN because they have considered only 10 number of nodes in their simulation study for the analysis of WSN performance.

A new MAC-layer protocol called Defeating Energy-Efficient JAMming (DEEJAM) [49] has been developed for defeating the hidden jammers with IEEE 802.15.4-based system. This security approach efficiently defeated several problematical and risky attacks such as activity jamming, interrupt jamming, pulse jamming and scan jamming. However, this protocol is applicable only for defending jammers but not considering other MAC layer attacks.

It is observed from the literature survey, various security mechanisms such as cryptography, encryption and secure routing protocols developed by various researchers to defend against wormhole and DDoS attack require more computational overhead, memory and energy consumption, so they are not more suitable for providing optimum energy and security for resource constrained network.

Subsequently, A.P. da Silva *et al* has proposed the traditional Decentralized IDS [50], which is the first and most cited signature or rule based IDS for WSN to identify the various

attacks in different layers. It is developed to identify the known type of attacks. The limitation of this kind of detection scheme is that it cannot identify the strange attacks or attacks having predefined property. Furthermore, maintaining the identity or signatures of attacks to make data base is a difficult task for WSN due to its inadequate memory and processing capacity. However, in very few literature surveys, this method has been explored by using watchdog approach [51]. Even though, this system identifies the various attacks in different layers, but high energy consumption required by monitor nodes makes it impractical for resource constrained ZigBee WSN.

Mati *et al* [52] pioneered the idea of watchdog and path-rate mechanisms. In this mechanism, every node implementing the watchdog is operated in promiscuous node, which constantly monitors the data forwarding behavior of its neighbors. 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 behaviors, whereas, watchdog detects a misbehaving node. However, weakness such as ambiguous collisions, limited transmission power, false behavior and collisions make this technique ineffective to be used for wireless sensor networks.

Onat and Miri [53] have developed a novel anomaly based intrusion detection security scheme for sensor networks having larger area coverage. It has been implemented by executing the low complexity anomaly detection algorithm at each sensor node separately, through which the detection and containment process is improved. The attack models which have been considered are node masquerade and resource depletion (Energy Exhaustion) attacks. In this security scheme, each sensor is capable of detecting the intruders by maintaining a statistical profile of its neighbor's behavior to monitor the power levels of received packets and their arrival rates. Since each sensor node contains the detection algorithm, it consumes high energy consumption which in turn leads to not suitable for a resource constrained wireless sensor networks. In addition, the system cannot identify wormhole attacks and selective forwarding due to the usage of simple statistics.

Numerous varieties of anomaly detection approaches [54-55] have been developed for wireless networks. Further, the anomaly detection approaches concentrate on the network layer only. In order to identify the attacks in other layers, a changes or modification is needed to design a new suitable technique particularly for resource constrained networks.

Chong Eik Loo *et al* [56] have presented intrusion detection for detecting routing attacks in sensor networks and claimed that, this system is able to detect the unknown attacks. In addition, many features used to make the normal profile is appropriate to make this system standard for identifying various types of attacks. Furthermore, the constant width clustering approach decrease the number of parameters necessary for clustering and requires only one pass through the network traffic samples. The main drawbacks of this system are high energy consumption due to IDS function performed by each node in the network independently and fixed width clustering algorithm with fixed distance threshold makes this system inflexible. Hence this system is unsuitable for resource constrained WSN.

I. Krontiris *et al* [57] have presented the misuse or signature based IDS to identify the known attacks by having the identity of the attacker, but due to the memory constraints of WSNs, misuse-detection based IDSs faces difficulties to store signatures of the attacker which makes the system likely to be less efficient. Further, misuse-detection techniques for WSNs with the help of watchdog approach have been investigated in various research articles.

Tran Hoang Hai *et al* [58] have developed a hybrid, lightweight IDS integrated for wireless sensor networks to detect the routing attacks in WSN. This IDS has used both anomaly and misuse techniques to detect the routing attacks and also used the advantages of cluster based protocol to form a hierarchical network. The detection of the attacks is achieved with the help of collaborative use of global agent and local agent integrated in the application layer of sensor node. However, this IDS is suitable only for cluster based network and the network lifetime is reduced due to more computational overhead required by cluster head.

Stetsko *et al* [59] have developed a neighbor based intrusion detection system for identifying various attacks such as jamming, hello flood and selective forwarding attacks to evaluate the system. Their system is executed for Collaboration Tree Protocol (CTP) on the TinyOS environment. Even though, the cooperation among nodes makes this system strong, the communication overhead is a major issue. In addition, the extracted features that are used to create the rules like packet transfer rate and packet dropping rate have caused a high false alarm to recognize attacks. Another disadvantage is that it did not consider the energy consumption rate which is a very serious problem in WSNs.

F. Nait-Abdesselam *et al* [60] have developed detection system for wormhole attack in wireless adhoc network with the aid of Optimized Link State Routing (OLSR) protocol. In this

approach, suspicious wormhole links are identified by exchanging probing packets between neighbors. However, this approach does not consume less energy due to the usage of control packets periodically for finding the suspicious wormhole link.

Zhibin Zhao [61] has developed an intrusion detection system based on statistical analysis to detect the wormhole for multipath routing. In this detection system, the wormhole link is identified by using drastic changes in statistics of routing message which is stored in the sink node. The statistical analysis includes determination of alleged link and validates the wormhole with time constraint. This system does not require any time synchronization and any special hardware, but the drawback of this system is that it works only for on-demand and multipath routing and fails to detect the hidden wormhole link.

Dezun Dong et *al* [62] have developed the distributed detection method for detecting the wormhole attack, which relies solely on network connectivity (Topology) information without any requirement of any hardware devices. This method identifies the wormhole based on topological message of the WSN. By detecting non-separating loops (pairs), this method can identify and locate various wormholes. It is suitable for continuous geometric surface where each node locally exchange message with neighbor and homogenous nodes. In this method four types of wormholes is classified based on their impacts on topology. Class-I wormhole is the malicious nodes that are located inside the surface. Class-II wormhole type has one end point inside the surface and the other end point exist on the boundary of the surface. In class –III type, two end points lies on different boundary. In class IV, the two end points of wormhole exist within the same boundary. The design of this detection method includes three components. They are candidate loop selection, finding independent non-separating loops, and seeking knit non-separating loop pairs. In candidate loop selection, shortest-path tree is established. Loop is constructed from two shortest paths and the threshold value is assigned for that loop. In finding independent non separating loop, when the candidate loop passes through the wormhole link, then the link is detected and locates two end points of the class-I wormhole and one end point of the class-II wormhole. In seeking Knit non-separating loop pair, class III or class-IV wormholes are detected by topological indistinguishable from a bridge across the candidate loop. Even though, this method has the advantage of detecting the exact single and multiples wormhole link in distributed environment, the complexity of detection scheme is high.

Forootaninia1 A. *et al* [63] have proposed an advanced watchdog technique for detecting the adversary nodes based on the power aware hierarchical model. In this watchdog approach, the cluster head act as a watchdog node. This storage overhead and buffer overflow are the issues faced by this mechanism because every message has to be managed by the cluster head. Among the existing works based on watchdog, Youngho Cho *et al* [64] have discussed about insider threats and their counter measures in wireless sensor networks. The major drawback of this approach is high energy consumption due to improper selection of watchdog node to monitor the network activities.

Further, detection mechanism for wormhole attacks in Delay-Tolerant Networks (DTN) [65] is developed. This approach exploits the existence of a forbidden topology in the network. Even though this, approach has detected wormhole attacks effectively in DTNs, it has achieved only 92% of detection rate.

Peng Zhou *et al* [66] have proposed Energy Efficient Trust System (EE-TS) using frequency and location optimization in watchdog approach to improve the performance of the Wifi based WSN in terms of energy and security. The main goal of this work is to enhance the security of the network to certain level of degree with less energy consumption. This approach consists of theoretical analyses and practical algorithms which are accomplished by scheduling the various tasks of the watchdog in view of the target nodes trustworthiness and location. This trust system is developed for detecting specific WSN attacks such as discrimination attack, bad-mouthing attack, on-off attack and sybil attack in wi-fi based WSN. However, this trust system can only applicable to wifi based WSN and it is unsuitable for resource constrained WSN due to extra energy consumed by the watchdog nodes. Further, the concept of optimized watch dog mechanism along with the consideration of energy consumption of nodes to choose watch dog nodes developed by Peng [66] is applied and investigated to develop the Energy Efficient Trust System for the detection of Wormhole attack (EE-TSW) in WSN. However, trade off between the energy consumption and performance metrics of IDS such as detection rate and detection time is not achieved.

Subsequently, various research works [68-69] have been developed by using Hidden Morkov Model (HMM) to predict the energy level of the senor nodes of WSN during different states and for speech recognition. However, the researchers have not used this model in the watch dog approach for the detection of attacks in the WSN. Hence, in order to improve the

performance of zigbee networks in terms of security and energy in the presence of attacks, the existing intrusion detection using watchdog are extended by incorporating watchdog location with optimization technique along with consideration of residual energy of nodes during the selection of watchdog nodes.

2.3. SUMMARY

In this chapter, state of the art literature review on security issues of routing attack in network layer and DoS attack in MAC layer for resource constrained wireless sensor network has been presented. It is evident from critical review of literature that exhaustive research works have already been done by several researchers to defend against various attacks to improve the WSN and ZigBee based WSN. Though security mechanisms such as cryptographic techniques, key management schemes and trust based routing protocols are developed to achieve better performance in the presence of attacks and they are not completely defending the particular attacks such as wormhole attack and DDoS (Energy Exhaustion) attack which in turn requires more memory and energy consumption and also more computational overhead. Further various IDS were extensively studied to get rid of the network from attacks and to enhance the network performance.

However, no attempt has been made so far to detect wormhole attacks to make the system energy efficient with better security by including optimized watchdog mechanism with the consideration of active monitoring technique along with the residual energy of watch dog nodes for detection of wormhole attack in the IDS system of ZigBee WSN by varying node density and attackers. Also the study of EE-IDS with different routing protocols such as AODV, STR and OSTR are yet to be explored to enhance the performance of ZigBee WSN in the presence of attacks. Further, no attempt has been made so far to detect DDOS attacks to provide the energy efficient security system by incorporating the optimized watch dog mechanism with the consideration of residual energy for watch dog nodes and normal nodes along with the HMM model for the detection of DDOS attack. Hence, an attempt has been made in the present research work to improve the performance of ZigBee WSN and IDS performance metrics by developing energy aware intrusion detection system for the above mentioned various protocols of ZigBee based WSN.

CHAPTER-3

ENERGY EFFICIENT INTRUSION DETECTION SYSTEM FOR DDOS ATTACKS

3.1 INTRODUCTION

The Energy Efficient Intrusion Detection System with Energy Prediction (EE- IDSEP) developed for Zigbee based Wireless Sensor Networks through simulation in order to detect MAC layer attack namely Distributed Denial of Service (DDoS) attacks is discussed in this chapter. Further, the performance metrics such as Packet Delivery Ratio (PDR), End-to-End Delay and energy consumption are determined and compared with that of existing Energy Efficient Trust System (EE-TS) [66]. Moreover, the metrics such as detection rate, False Positive Rate (FPR) and detection time of proposed EE-IDSEP are also examined to evaluate the efficiency of the proposed system.

3.2. DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

Most devices in LR-WPAN are resource-constrained and lack physical safeguards due to the deployment of nodes in harsh environment. Hence, the important resource of nodes like energy can be influenced or exhausted or by DDoS attacks easily. Typically, the DDoS attack includes resource depletion attack, energy exhaustion attack and flooding. Generally, DDoS attacks are distinct as attacks launched from several ends of a wireless sensor network towards target legitimate sensor nodes, with the aim of draining their limited energy resources. These attacks can extensively influence the performance of the WSN, and ultimately, compromise the entire network completely. If the DDoS attacks are undetected in the network, it may cause disastrous to the entire network operations. As a result of this attack, the target node is inundated with huge number of requests than its maximum processing capability, thus interrupt or blocking the further services provided by the sink or coordinator to its clients. More exclusively, distributed denial of service attacks may possibly go ahead to exhaust the energy resources of a legitimate target node. It also refers to distributed energy-exhaustion in WSN, which is achieved by sending continuous requests to the target sensor node from the multiple attacker nodes to exhaust the energy of the target sensor nodes.

Generally, these malicious nodes consume extra energy to launch DDoS attacks. In this work, the energy exhaustion attack is considered as the DDoS attack. Hence, it is required to predict the energy consumed by sensor node at various states in order to identify the malicious nodes in the network. For this, energy dissipation rate of sensor nodes is determined by using the Hidden Markov Model (HMM) [68-69] which is used in the proposed EE-IDSEP to detect DDOS attack.

3.3. PROPOSED EE-IDSEP FOR DETECTION OF DDOS ATTACK

The functional flow diagram of proposed system EE-IDSEP is shown in the figure 3.1. It comprises of three main stages; they are topology discovery by sink / coordinator, optimized location of watchdog nodes and DDoS attack detection. The procedure or method involved in topology discovery by sink and optimized location of watchdog nodes is described in the following section. The heart of the proposed system EE-IDSEP is detection of DDoS attack function which is done by HMM for estimation of energy dissipation rate of sensor nodes that is described in the following section.

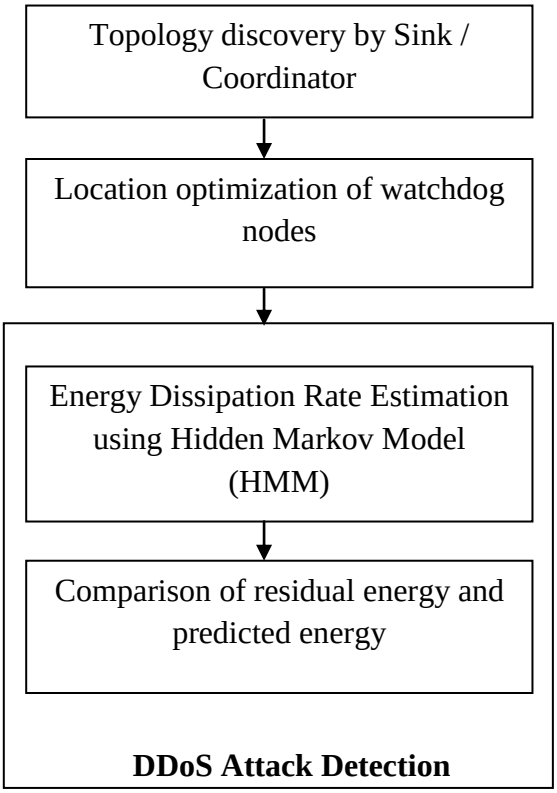


Figure 3.1 Functional flow diagram of proposed system EE-IDSEP

3.3.1. Topology Discovery

In this phase, the sink node discovers the network topology by broadcasting a topology message periodically to entire sensor nodes in the wireless network. After the topology message is received, QoS metrics like residual energy (E_R) and Queue Delay (QD) of its neighbor nodes are measured by every node in the network. Further, every node collects the data about other nodes and stores in a Topology Information Table (TIT) as shown in table 3.1 after the measurement of above-mentioned QoS metrics.

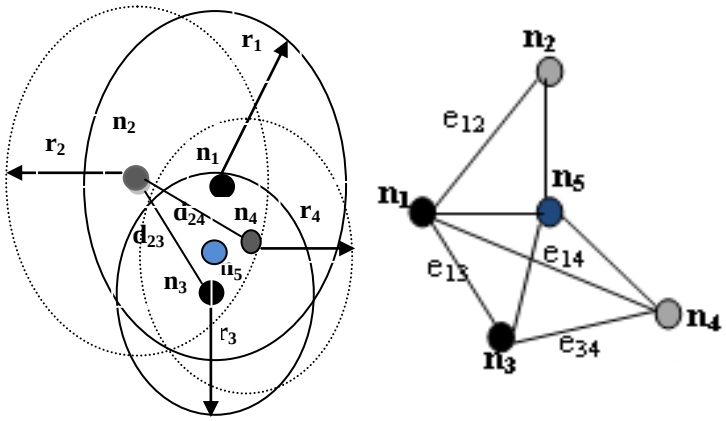
Table 3.1Topology Information Table (TIT)

Source Node ID	1-hop neighbour node ID	2-hop neighbour node ID	Residual Energy (E_R)	Queue delay (QD)

Thus, TIT contains the source node ID, 1-hop and 2-hop neighbor node ID, residual energy(E_R), and QD of each node along with the 2-hop neighborhood information. Finally, the TIT value is broadcasted again towards the coordinator or sink by the nodes for updating the information of the nodes in the network.

3.3.2. Location Optimization of Watchdog Nodes

The WSN with flat topology is demonstrated with the system model of M = (N, E) referred from the existing system [66] that is illustrated in figure 3.2. In this figure, $n_i \in N$ indicates a sensor node in WSN and $e_{ij} \in E$ denotes that the nodes n_i and n_j are neighborhood nodes (i.e., which are existed within each other's communication range). Let r_i is considered to be the communication range of n_i, and d_{ij} is the spatial distance between n_i and n_j. Consider $e_{ij} \in E$ exists only if $d_{ij} \leq r_i$ and $d_{ij} \leq r_j$.. Let $B_i = \{n_j | e_{ij} \in N\} = \{n_j \mid d_{ij} \leq r_i \,\&\, d_{ij} \leq r_j\}$, $B_i \in N$ is defined as the set of n_i's neighborhood nodes. Even though, n_3 and n_4 present within n_2's communication range (i.e., $d_{23} \leq r_2$ and $d_{24} \leq r_2$), but e_{23} and e_{24} do not survive (i.e., n_3, $n_4 \notin B_2$) because $d_{23} > r_3$ and $d_{24} > r_4$. The location of watchdog nodes are optimized by reducing the energy cost of the complete WSN and also improving the security in terms of trust worthiness, detection rate, False Positive Rate (FPR) and detection time. To achieve optimization, a proper set of cooperative watchdog nodes (W_j) is to be identified. This problem is to choose the nodes from each target neighbor nodes to carry out the watchdog task and to schedule the watchdog tasks among those chosen watchdog nodes.



WSN M= (N, E)

Figure 3.2 WSN with the system model M

The node n_i can function as a watchdog to monitor n_j only $\forall nj \in Bi$, and vice versa. The nodes that are placed close to the optimal distance d_{ij} and having highest residual energy with maximum number of neighbor nodes must be elected as watchdog nodes. Hence, the problem of finding out optimal watchdog node W_j can be transformed to the problem of finding optimal d_{ij}. The node n_i with less d_{ij} will consume less energy compared to the nodes that are located farther apart which in turn leads to achieve higher residual energy. In case, if adversary nodes are selected as watchdogs, then the security goal is not attained. Hence, the determination of optimal watchdog location d_{ij} is done by taking into consideration of the overall risk, which considers both security and energy consumption. Hence, the node n_5 is selected as the watchdog node (W_5) based on the above conditions, which is shown in figure 3.2.

3.3.3. Energy Dissipation Rate Estimation using Hidden Markov Model

The HMM is an expansion of the conventional markov model referred from the existing system [68-69]. In HMM, the final state of the process is only observed but the Markov process is not visible (i.e.), it is hidden. There are different states adopted in HMM. They are the initial state, transition state and observed state. Based on the different possible outcomes, every state has probability distributions. The sequence followed by the process is hidden but not the observed state. HMM consists of set of hidden states *S* and set of observation states *V* which is illustrated in figure 3.3. The set of hidden and observed states are expressed in equations 3.1 and 3.2 respectively.

$$S = (s1, s2 , s3 , ..., sn) \quad (3.1)$$

$$V = (v1, v2 , v3 , ..., vm) \quad (3.2)$$

Q is considered to be the state sequence of fixed length L, for corresponding observations O,

$$Q = q1, q2 , q3 , ..., qL \quad (3.3)$$

$$O = o1, o2 , o3 , ..., oL \quad (3.4)$$

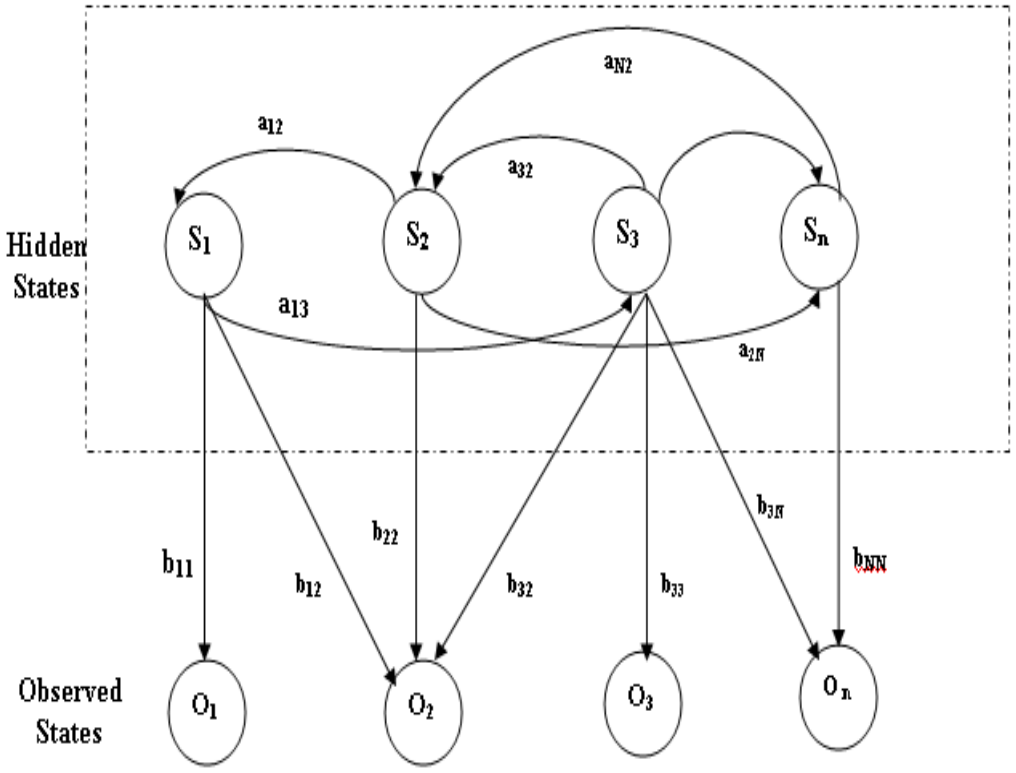


Figure 3.3 Hidden Markov model

HMM is generally expressed as,

$$\lambda = (A, B, \pi) \quad (3.5)$$

Where 'A' denotes the state transition probability matrix, 'B' denotes the observation matrix and 'π' denotes the initial state distribution. The various states of sensor nodes are denoted by TRANSMIT (T), RECEIVE (R), PROCESS (P) and IDLE (I).

Further, *A* indicates the state transition array, that is independent of time *t* and keeps track of probability of interference state *j* following interference state *i* and it is indicated as below,

$$A = [aij\ ],\ aij = P(qt = s\,j \mid qt{-}1 = si\ ) \tag{3.6}$$

The corresponding state transition matrix of A is given by

	I	T	R	P
I	0.4	0.3	0.2	0.1
T	0.3	0.4	0.2	0.1
R	0.2	0.1	0.3	0.4
P	0.4	0.3	0.1	0.2

(3.7)

Here, A denotes the probability of changing from one state to another. For example, the probability of changing from T to R is given by P(T | R)=0.2. Similarly, P(I | P)=0.1, P(R | P)=0.4.

Then, B denotes array of observation and it is independent of time *t*. It stores the probability of observation *k* that is produced from the state *j*. The observation array *B* is given in equation (3.8)

$$B = [bi\ (k)],\ bi\ (k) = P(xt = vk \mid qt = si\ ) \tag{3.8}$$

The matrix B is given by

	L	M	H
I	0.5	0.3	0.1
T	0.1	0.4	0.5
R	0.3	0.3	0.4
P	0.2	0.4	0.4

(3.9)

Where L (Low), M (Medium) and H (High) denote the range of values used to determine the Energy Dissipation Rate (EDR). B denotes the probability of L, M and H for the 4 states

Here, the different states of a power consumed during different states of a sensor node such as TRANSMIT, RECEIVE, PROCESS and IDLE are also corresponded to observation states. The corresponding powers like TxP, RxP, PrP and IP represent transmit, receive, processing power and idle power, respectively at N time intervals. The output (hidden state) is the cumulative energy dissipation rate of the corresponding nodes over the N time intervals.

Further more, π signifies the initial state probability as shown below,

$$\pi = [\pi i\ ],\ \pi i = P(n1 = Ii\ ) \quad (3.10)$$

π is given by

I	T	R	P
0.4	0.3	0.2	0.1

(3.11)

Here π denotes the initial probability distribution for the 4 states. The probability of the state sequence X is given by

$$\pi 1.\ b1(H).a1(I \mid T) \times \pi 2.\ b2(L).a2(T \mid R) \times \pi 3.\ b3(M).a3(R \mid P) \quad (3.12)$$

Where b1, b2, b3 represent the elements of matrix B and a1, a2, a3 represent the elements of matrix A. Then, from equations (3.7), (3.9) and (3.11), eqn (3.12) becomes

(0.4) (0.1) (0.4) x (0.3) (0.1) (0.2) x (0.2) (0.3)(0.4) = 0.00000576

Similarly, the state sequence probability for any set of observation sequence of EDR can be found.

3.3.4. Detection of DDos Attack

The detection of the DDoS attack is described in the form of flowchart shown in the figure 3.4. The detection of the DDoS attack is done by using the Hidden Markov Model (HMM) scheme to estimate the energy consumption by the sensor nodes. The energy dissipation rate of sensor nodes is calculated by applying the HMM.

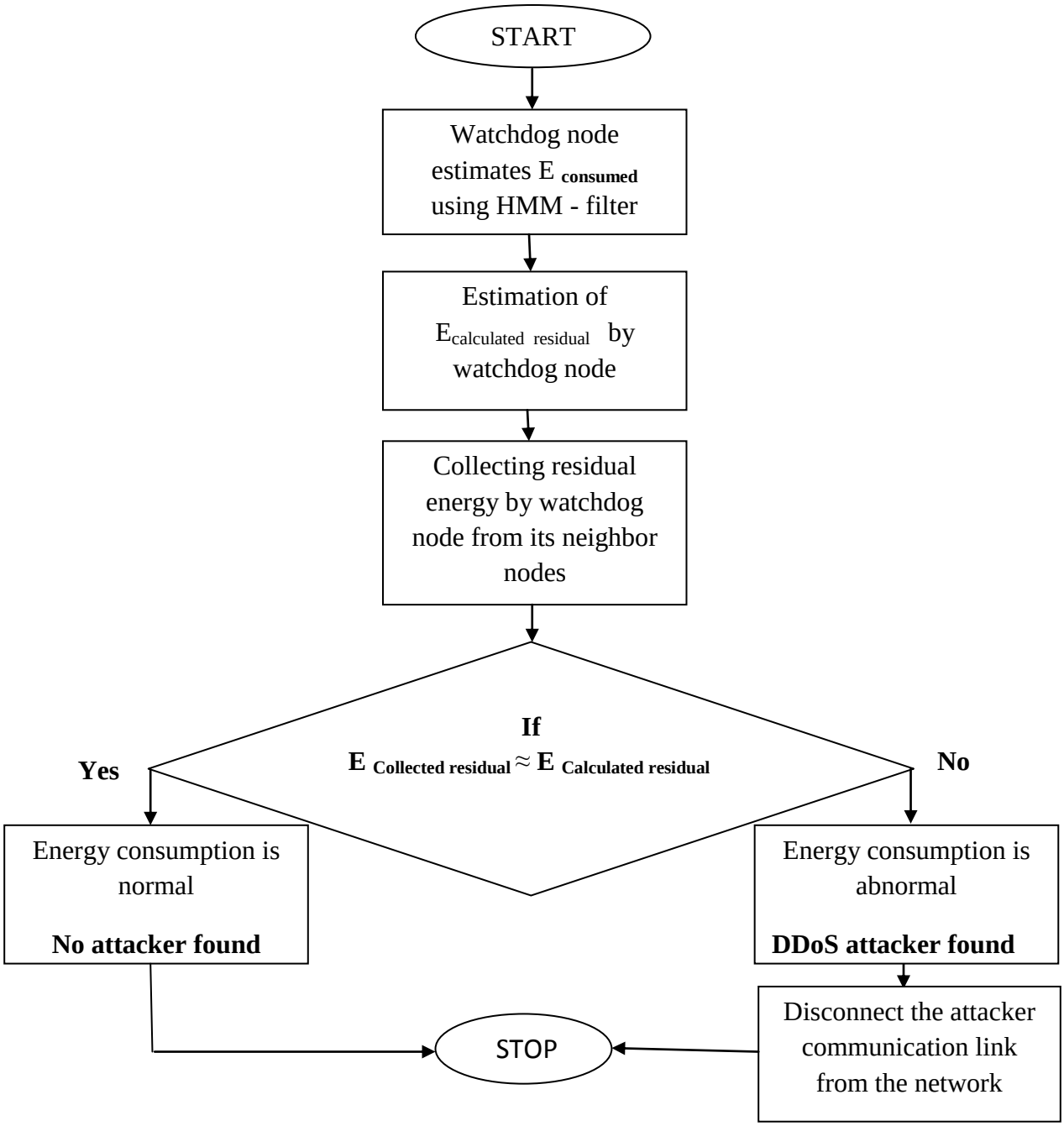


Figure 3.4 Flowchart for the detection of DDoS attack

At first, the watchdog nodes estimate the $E_{consumed}$ by using HMM filter. Next, watchdog nodes collect the residual energies from all monitored nodes. Then, the difference between the initial energy and $E_{consumed}$ is estimated by watchdog inorder to calculate the $E_{Calculated\ residual}$ and compares them with collected residual energy ($E_{\ Collected\ residual}$) from all the monitored nodes. If the watchdog observes the huge difference in the energy consumption level, then, the occurrence of the DDoS attack is detected which indicates that the node is malicious. Thus, the DDoS attack is identified efficiently in the network and finally, the communication link with the attacker node is removed from the network. The nodes with abnormal energy consumption are considered to be DDoS attacks with the aid of HMM in the EE-IDSEP method.

Algorithmic steps for detection of DDoS attack

The notations used in the algorithm are given below.

- **$E_{\ consumed}$** : Estimated Energy dissipation rate of various states using HMM
- **$E_{\ Collected\ residual}$**: Collected residual energy from the monitored nodes.
- **$E_{\ Calculated\ residual}$** : Estimated residual energy by watchdog node based on **$E_{consumed}$** and Initial energy

The algorithm steps are as follows:

Step 1: Watchdog node estimates $E_{\ consumed}$ by using HMM filter

Step2: Watchdog estimates the **$E_{Calculated\ residual}$** (difference between the **initial energy** and $E_{\ consumed}$ **)**

Step3: The watchdog collects the residual energy (**$E_{\ Collected\ residual}$**) from all the monitored nodes

Step 4: If **$E_{\ Collected\ residual} \approx E_{\ Calculated\ residual}$** , then energy consumed is normal

Step 5: If **$E_{\ Collected\ residual} \neq E_{\ Calculated\ residual}$** , then energy consumed is abnormal

Step6: If energy is abnormal then attacker node link will be disconnected from the network else go to step 1.

3.4. SIMULATION RESULTS AND DISCUSSION

The effectiveness of proposed approach is examined in terms of PDR, average end-to-end delayand energy consumption by varying number of DDoS attacks and detection rate, false positive rate as well as average detection time by varying node density in presence of attacker.

Finally, the simulation results of the proposed system namely EE-IDSEP is compared with the existing EE-TS. NS2 simulator is used to stimulate the proposed and existing IDS [66]. The parameters and corresponding values used in this simulation are listed in the table-3.2. Figure 3.5 depicts the Zigbee based WSN scenario with DDoS attacks.

Table 3.2 Simulation Parameters for EE-IDSEP

No. of Nodes	25, 50, 75, 100
MAC	IEEE 802.15.4
Area	100 X 100 m^2,
Routing Protocol	AODV
Attackers (DDoS attack)	5 no's
Traffic Source	Poisson
Simulation Time	100 sec
Initial energy of node	1 Joule
Propagation	Two Ray Ground

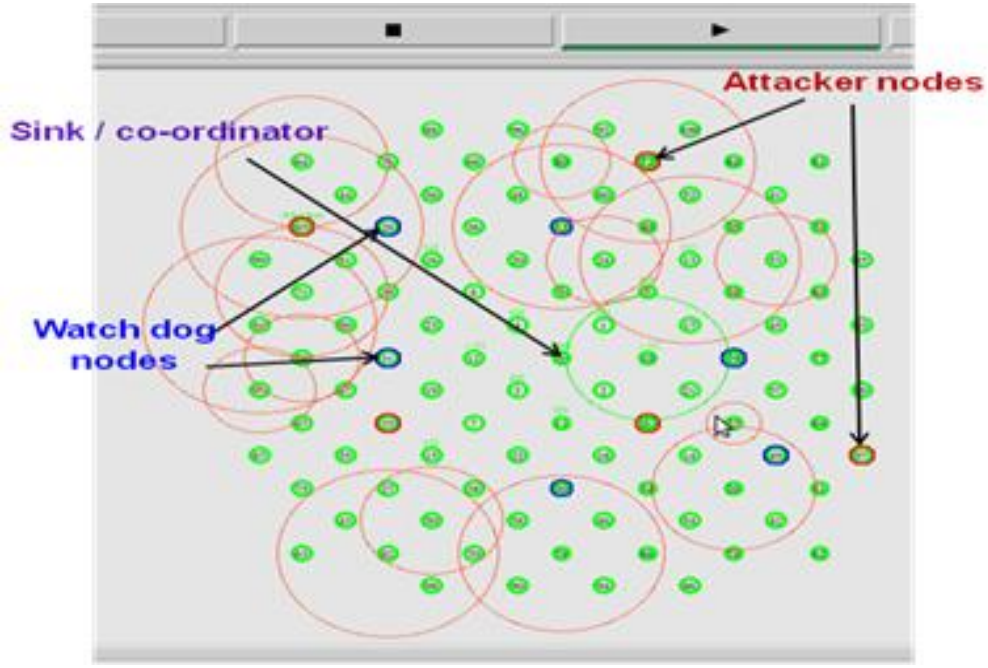


Figure 3.5 ZigBee WSN scenario with DDoS attacks

The ZigBee wireless sensor network consists of 100 numbers of nodes deployed randomly over the terrain area of size 100 x 100 m^2. The DDoS attacker nodes are deployed randomly into the formed networks which are indicated by nodes circled with red color. Blue color nodes that are selected by the sink or coordinator based on certain condition as explained in the previous section 3.3.2 represent watchdog nodes. The center node is a sink or coordinator node indicated in green color as normal nodes.

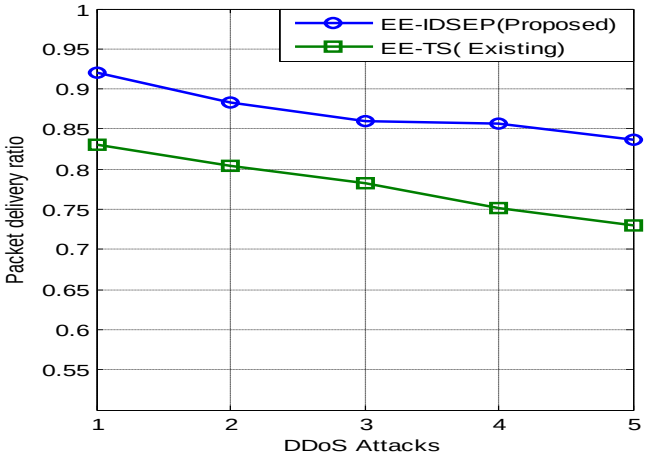


Figure 3.6 Packet delivery ratio Versus Attacks

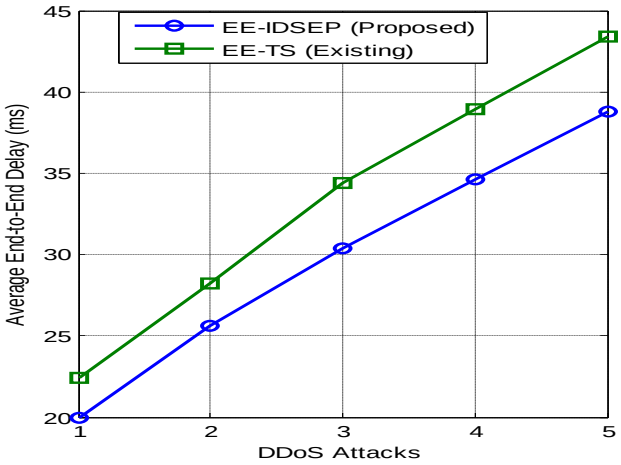


Figure 3.7 Avg. End-to-End Delay Versus Attacks

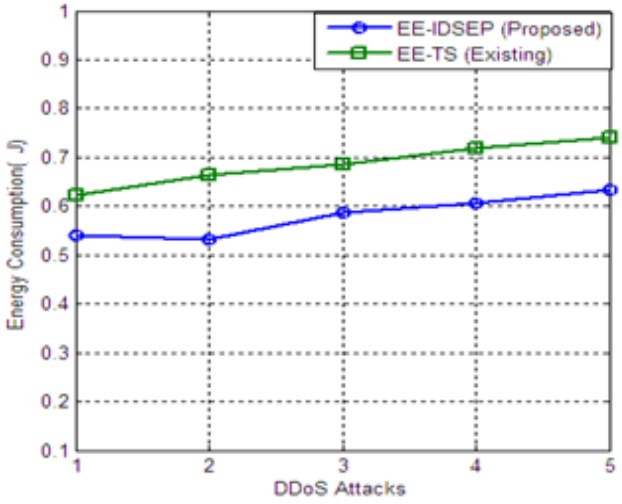


Figure 3.8 Energy consumption Versus Attacks

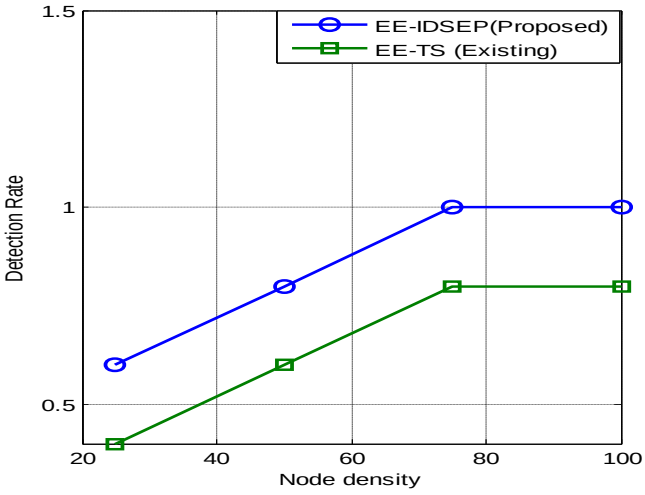
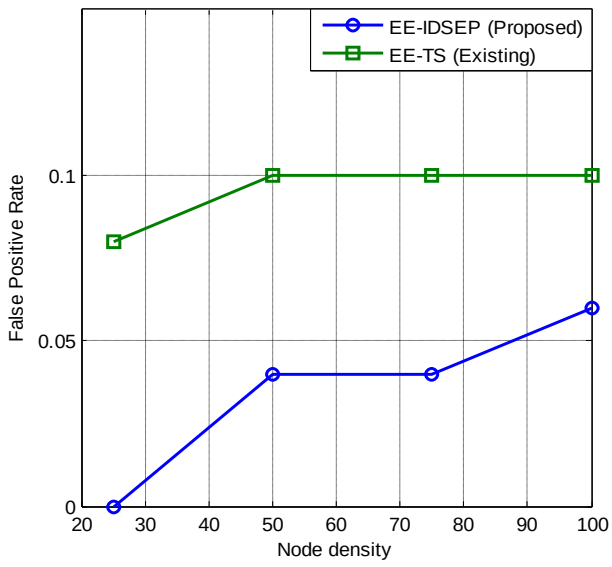


Figure 3.9 Detection rate Versus Node density

The simulation results shown from the figure 3.6 to 3.8 depict the packet delivery ratio, average end-to-end delay and energy consumption with respect to number of DDoS attacks. It is evident from the figure 3.6 that PDR decreases with respect to increased DDoS attacks due to the

influence of attackers on the normal nodes. Also, it is inferred from the simulation result that EE-IDSEP is better than that of existing EE-TS by providing approximately 12% improvement in terms of PDR. Figure 3.7 portrays that average end-to-end delay is increased w.r.t increased number of DDoS attacks, but comparatively EE-IDSEP achieves the improved performance in terms of reduced average end-to-end delay by approximately 10%. Further, the proposed EE-IDSEP provides improved reduction in energy consumption than that of the existing EE-TS by approximately 15% as depicted in fig. 3.8.

Further, fig. 3.9 to 3.11 illustrates the IDS performance metrics such as detection rate, False Positive Rate (FPR) and average detection time of proposed and existing system. Detection rate is the ratio of intrusion instances detected by the system to the total number of intrusion instances present in the test set. FPR refers to the prediction of normal nodes as attackers. From the simulation results, it is proved, that the proposed EE-IDSEP achieves 33.3% of enhancement in detection rate, 22.5 % of reduction in detection time than that of existing system and EE-IDSEP also achieves 4.6% of False Positive Rate (FPR).



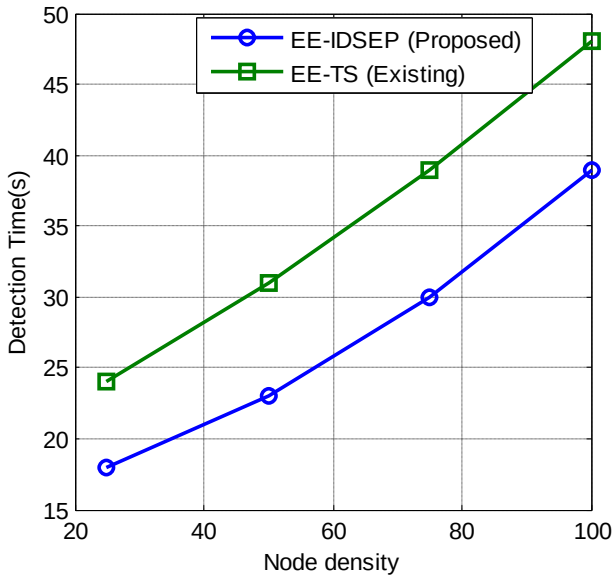


Figure 3.10 False Positive Rate Versus Node density

Figure 3.11 Detection time Versus Node density

The overall enhancement in the above-mentioned performance metrics is achieved by EE-IDSEP compared to that of existing system. The reason is that effect of attackers is reduced quickly after detecting the attacker nodes and also their corresponding link is eliminated from the

network by using coordinator in the proposed EE-IDSEP with the aid of optimized watchdog nodes.

3.5. SUMMARY

In this chapter, EE-IDSEP is developed for Zigbee based WSN to detect the DDoS attack. The performance of Zigbee based WSN using proposed EE-IDSEP such as PDR, average end-to-end delay, energy consumption, detection rate, false positive rate and detection time are determined and compared with EE-TS. It is portrayed through the simulation results that the EE-IDSEP achieves better performance metrics than that of existing system.

CHAPTER-4

ENERGY EFFICIENT INTRUSION DETECTION SYSTEM WITH AODV ROUTING PROTOCOL

4.1 INTRODUCTION

In this chapter, the Energy Efficient Intrusion Detection System (EE- IDS) with Adhoc On demand Distance Vector (AODV) protocol developed through simulation for Zigbee based wireless sensor networks in order to detect wormhole attacks is described. Then, the performance metrics such as Packet Delivery Ratio (PDR), end-to-end delay, and energy consumption are determined and compared with that of existing Energy Efficient Trust system for wormhole detection (EE-TSW) [66]. In addition to this, the metrics of IDS such as detection rate, FPR and detection time of proposed EE-IDS are also determined to evaluate the efficiency of the proposed system.

4.2. WORMHOLE ATTACK

One of the most common and dominant attacks in the network layer is wormhole attack [17]. In this attack, an adversary or malicious node form a high bandwidth tunnel between the source and destination in order to provide superior communication resources to the nodes when compare to the normal sensor nodes. The wormhole attack also tunnels the packet received in one part of the network over a low-latency link. Then, it replays them in various part of the network through a private channel. Routing between source node and destination node through the private channel provided by wormhole attack is selected due to the requirement of lesser number of hops or less latency in that route compared to that of packets sent through the other normal routes. The adversary nodes situated close to the base station can be able to interrupt the routing information completely by forming well-placed wormhole nodes W1 and W2 as shown in figure 4.1.

The packets sent by node N1 may reach the destination node N6 via normal route (N1-N2-N3-N4-N5-N6) and also through the route formed by wormhole nodes W1 and W2. The packets that follow the normal route reach destination node N6 later than those transferred through the wormhole route. Therefore, packets are dropped because normal route requires more

hops. Thus, the wormhole node attracts the packets by forming false routing information between source and destination.

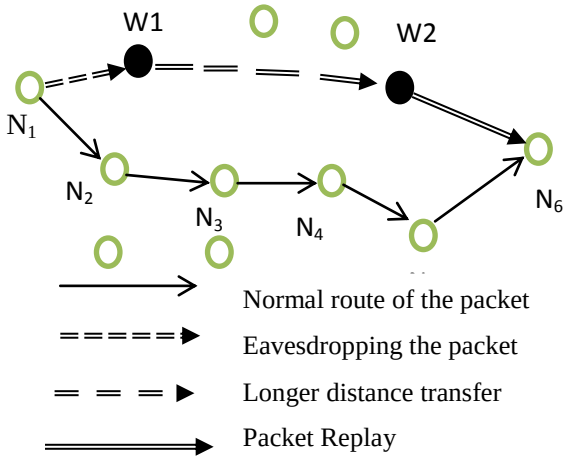


Figure 4.1 Wormhole attack

The packets tunneled by the wormhole nodes are mishandled by breaking the encryption key, altering the content of packets and dropping the packets to make the communication failure with each other or send the data to a third party for corrupting the information of the packets. Wormholes are hard to detect and can strongly influence the performance of network services such as localization, data fusion and time synchronization. This attack also forms a serious threat in wireless networks, especially against routing protocols of wireless networks.

4.3. AODV ROUTING PROTOCOL

The AODV routing protocol [67] proposed for Mobile Ad hoc NETwork (MANET) and sensor networks is prone to various attacks such as sink hole and wormhole attacks. AODV uses on-demand approach for finding routes, (i.e), a route is recognized only when a source node is required to transmit the data packets to the destination node, hence it is known as reacting routing protocol. AODV uses Route REQuest (RREQ), Route REPly (RREP) and Route ERRor (RERR) messages to locate and maintain the routes. AODV consists of two fundamental operations, which are route discovery and route maintenance. In route discovery, a RREQ packet is broadcasted when a destination node does not have a route from the source node. Typically, RREQ packet contains source IP address, destination IP address, source sequence number,

destination sequence number, hop count and request ID. The RREQ packet will be discarded, when a route request with the same source address and request ID is received by a node as those in one of the earlier routes request packets. Otherwise, the RREP is forwarded back to the source node through the route, when the route request with the new sequence number is received. In route maintenance, if a link breakage is found in an active route, the node reports this link breakage by transfer a RERR packet to the source node. The source node will again initiate the process of route discovery if it still has the message to send.

4.4. PROPOSED ENERGY EFFICIENT INTRUSION DETECTION SYSTEM WITH AODV ROUTING

In the proposed system EE-IDS-AODV, the technique namely optimized watchdog trust system is used for detecting the wormhole attacks. Figure 4.2 illustrates the typical architecture of IDS known as EE-IDS-AODV in addition to the sensing and data transmitting capabilities.

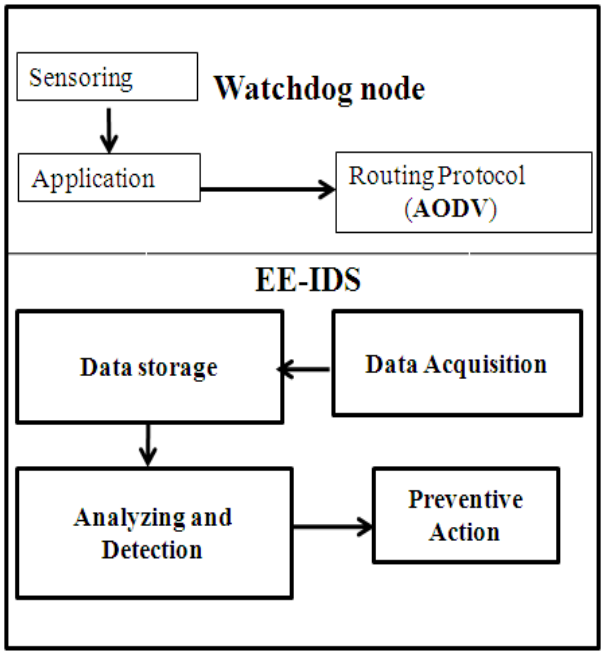


Figure 4.2 Architecture of EE-IDS-AODV

The proposed EE-IDS is a signature based IDS technique. It has three main phases; they are (i) Data acquisition: In this phase, data's are gathered in a promiscuous mode to sort out the vital data before data storage. Mostly it will monitor the traffic pattern, internal events and resource utilization of the neighbor nodes. (ii)Next phase is analysing and detection stage, where pre-defined rules are applied to the data stored in the memory for analysing and detecting the

intruders. If any abnormalities are present, the decision is taken based on the threshold value whether the node is malicious or not. (iii) Final stage is preventive action phase, which is meant for taking preventive measures against the attack, which is done by the administrator node or co-coordinator of the network with the help of watchdog node.

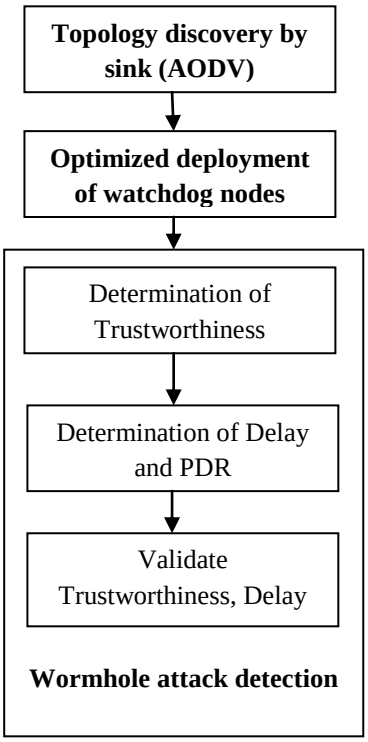


Figure 4.3 Functional flow diagram of proposed EE-IDS-AODV

The functional block diagram of proposed EE-IDS-AODV is illustrated in figure 4.3. It consists of three main phases. They are topology discovery, optimized deployment of watchdog nodes and detection of wormhole attack. The sink node conducts the topology discovery phase in order to make out the routing path from every node to the coordinator or sink that is stored in the respective nodes. In this phase, the routing protocol namely AODV is used for routing the packets. Further, topology discovery phase follows the same function as discussed in the section 3.3.1 of chapter- 3. Following the topology discovery phase, optimized deployment of watchdog nodes is done, which is clearly explained in the section 3.3.2 of chapter-3. Finally, the wormhole attack detection is done based on determining the three factors such as trustworthiness of the

nodes, the abnormal deviation in the PDR and end-to-end delay. Here, each watchdog node determines the trustworthiness of the nodes in the network by collecting the hop by hop QD and received traffic.

4.4.1. Detection of Wormhole Attack

The active and passive detection techniques are combined and then they are applied to detect wormhole attack. In the passive technique, extra data traffic is not appended into the network. But, the attack is identified on the basis of the abnormalities detected by the passive monitoring method. In the active method, regular search traffic is sent into the network to collect the end to end statistics so that the validity of the network is accordingly decided to deduce the network health

The important parameters considered for the detection of wormhole attack are node trustworthiness, the abrupt variation in the end to end delay and PDR. The most stable nodes in the network (a node which is having the highest residual energy and more neighbor nodes) are chosen as the watchdog nodes. The hop by hop queuing delay is the significant delay experienced by a data packet at each node as it waits for its turn, to be send to the next node along the path to its destination. The node experiencing end-to-end delay lesser than minimum threshold value is suspected as attackers. Finally, in proposed approach, the wormhole verification is performed on such suspicious links by exchanging control packets such as $HELLO_{req}$, $HELLO_{rep}$, probing packet and $ACK_{prob.}$

The trustworthiness (T_{ij}) is measured by watchdog node as given below.

$$T_{ij} = \frac{\sum_{t \in T \vee w^{t}_{ij} \neq \emptyset} K^{t}_{ij}}{\sum_{t \in T \vee w^{t}_{ij} \neq \emptyset} 1} \qquad (4.1)$$

Where,

w^{t}_{ij} : The watchdog task is performed by n_i to monitor n_j at time slot t

K^{t}_{ij} : The event to represent n_j's behaviour that is expected by n_i at time slot t.

T : Time window

The Event K^{t}_{ij} returns 1, if n_i expectation is satisfied by n_j's behavior, otherwise it will return 0.

The equation for end to end delay (D) is given below.

$$D = N [D_{Tran} + D_{prop} + D_{Proc}] \quad (4.2)$$

Where,

N : Number of links (number of routers +1)

D_{Proc} : Node processing time to accept and forward a packet to the specific node

D_{prop} : Time taken to travel through all the links

D_{Tran} : Transmission Delay (i.e)

$$D_{Tran} = L/R \quad (4.3)$$

Where, L is the number of bits in the data packet and R is the data transmission rate

The equation for PDR is given by

$$PDR = \frac{\text{Total Packets Received}}{\text{Total Packets Sent by source}} \quad (4.4)$$

The following flowchart illustrated in figure 4.4 describes the wormhole detection technique used in the proposed system EE-IDS-AODV. The notation used and algorithmic steps for the detection of wormhole is explained as follows.

Notations used:

- *D* : End To End Delay
- $D_{Watchdog}$: End to end delay predicted by the watchdog
- W_N : Watchdog node
- D_{Sink} : End to end delay predicted by the sink
- *TD* : Topology Discovery
- $PDR_{Watchdog}$: PDR predicted by the watchdog
- PDR_{Sink} : PDR predicted by the sink

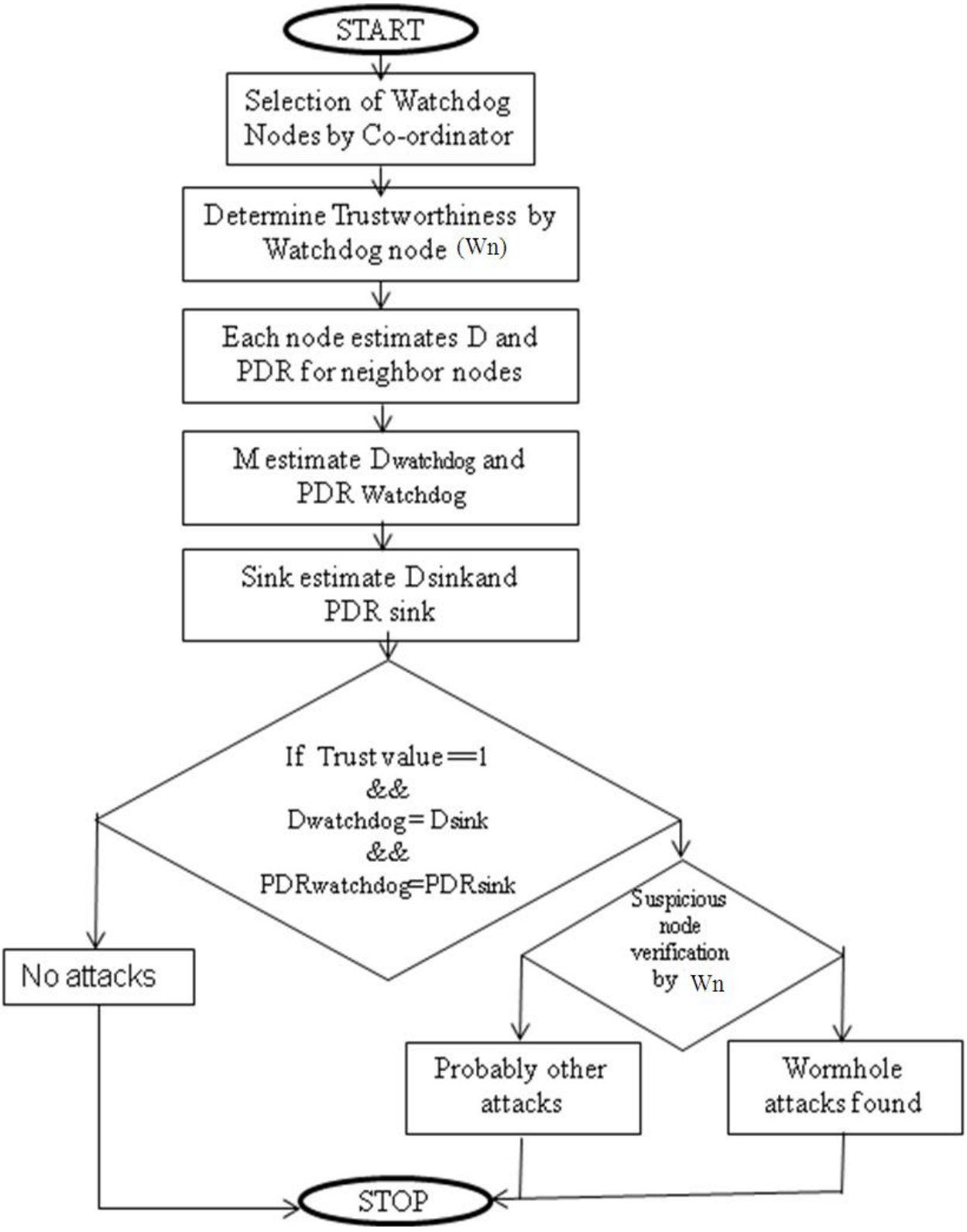


Figure 4.4 Flowchart for wormhole detection

Algorithm for Wormhole Detection:

i. The selection of watchdog is done by sink/Coordinator node.
ii. The watch dog W_N determines the trustworthiness of each node in the network based on the hop by hop queuing delay and received traffic.
iii. Each node send probes to its 2 hop neighbours and records the average *D*, also estimates the *PDR* along the path between the 2 hop nodes.
iv. W_N collects the recorded values at regular intervals of time.
v. Based on the received values, W_N ensures the trustworthiness of each node by correlating the values get from different nodes and also estimates a practical $D_{Watchdog}$ and $PDR_{Watchdog}$ value experienced by the data packet.
vi. The sink executes *TD* using the *TD* agents and records the observed statistics in respect of *D* and *PDR* after receiving the data packet.
vii. The dependency between the nodes and end to end paths are determined based on the observed statistics. And, the D_{Sink} and PDR_{Sink} value is estimated.
viii. Then the sink compares the values estimated by it, with the values estimated by W_N.
ix. If $D_{Watchdog} = D_{Sink}$ && $PDR_{Watchdog} = PDR_{Sink}$ && trustworthiness = 1, then no attack is detected.
x. If $D_{Watchdog} \neq D_{Sink}$, or/and $PDR_{Watchdog} \neq PDR_{Sink}$&& trustworthiness $\neq$ 1 then wormhole attack is suspected. Finally, the suspicious link is verified by timeout parameter calculated by using exchanging control packets between the suspicious node and W_N.
xi. If trustworthiness, Delay and PDR are in normal value, then there is no attack. If they are not in normal value then the wormhole attack is identified.
xii. Finally, after detecting the wormhole attacks, the communication link of wormhole nodes is disconnected from the network to mitigate the effect of attacks completely.

4.5. SIMULATION RESULTS AND DISCUSSION

The performance of proposed approach is examined in terms of packet delivery ratio, average end-to-end delay, energy consumption by varying number of wormhole attacker and detection rate, false positive rate as well as average detection time by varying node density.

Finally, the simulation results of the proposed system namely EE-IDS with AODV is compared with the existing EE-TSW.

The parameters used for this simulation are listed in the table-4.1. Figure 4.5 depicts the ZigBee WSN scenario with wormhole attacks. It consists of 100 number of nodes deployed randomly over the terrain area of size 100 x 100 m^2. The wormhole attacker nodes are deployed randomly into the formed ZigBee networks, which are indicated by nodes circled with red color. The blue color nodes are watchdog nodes selected by the sink or coordinator based on certain conditions as explained in previous section. Sink node is a center node indicated in green color as that of normal nodes

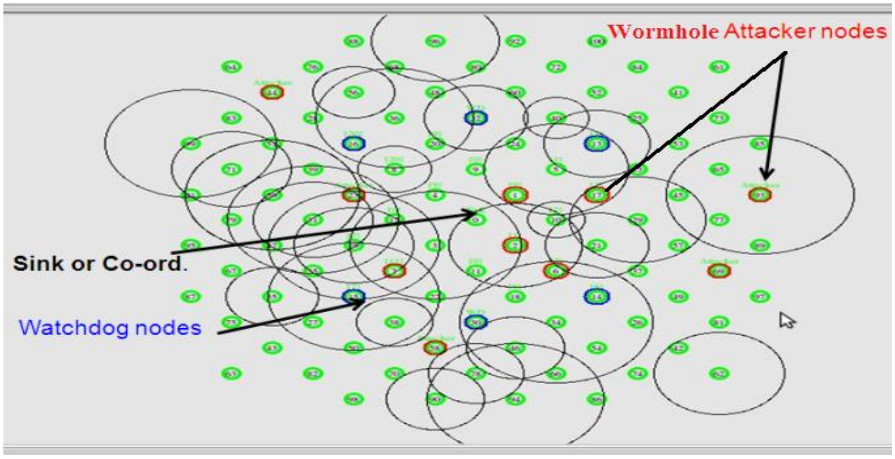
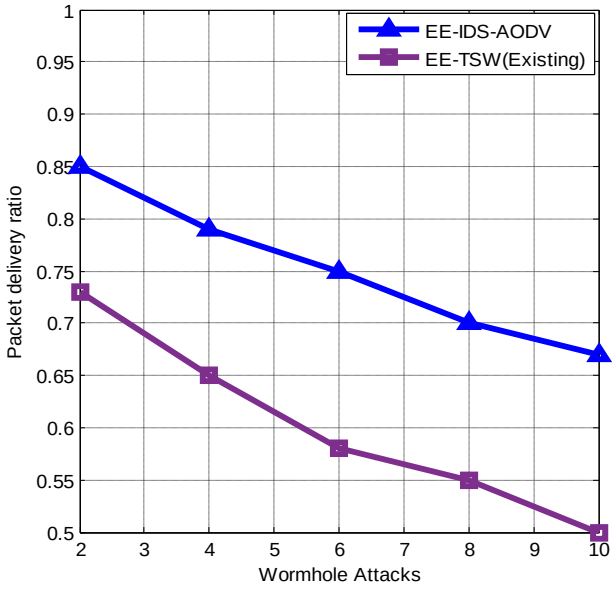


Figure 4.5 ZigBee WSN scenario with Wormhole attacks

Table 4.1 Simulation Parameters for EE-IDS-AODV

No. of Nodes	25, 50, 75, 100
MAC	IEEE 802.15.4
Routing Protocol	AODV
Area	100 X 100 m^2,
Simulation Time	100 sec
Attackers (Wormhole)	5 pairs of attackers
Initial energy of node	1 Joule
Traffic Source	Poisson
Propagation model	Two Ray Ground

This section illustrates the simulation results of proposed EE-IDS-AODV and existing EE-TSW. The simulation results shown from the figure 4.6 to 4.8 depict the packet delivery ratio, average end-to-end delay and energy consumption with respect to number of wormhole attacks.



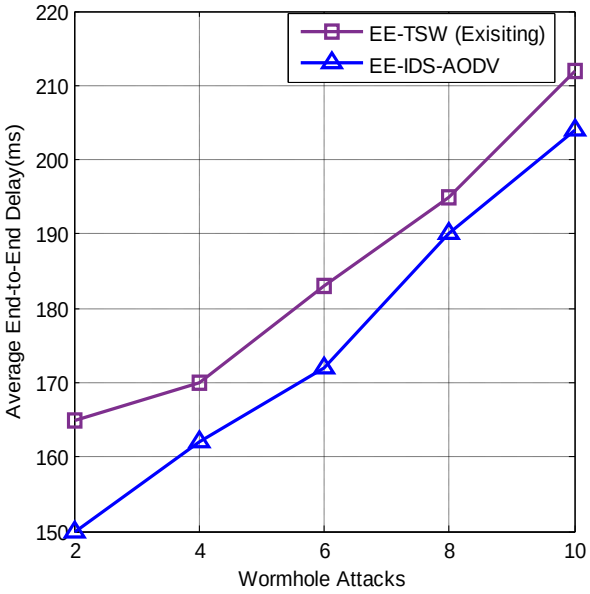


Figure 4.6 Packet delivery ratio Versus Attacks

Figure4.7 Avg. End-to-End Delay Versus Attacks

It is portrayed from the fig. 4.6 that PDR decreases w.r.t increased wormhole attacks. Also, it is inferred from the above mentioned result that proposed IDS namely EE-IDS-AODV achieves better PDR performance than the existing EE-TSW by approximately 23%. It is depicted through the fig.4.7 that proposed EE-IDS-AODV shows the improved performance in terms of reduced average end-to-end delay by approximately 5.4% compared to that of existing system.

Further, the proposed EE-IDS with AODV achieve improved reduction in energy consumption than that of the existing EE-TSW by 4.3% as depicted in fig.4.8. The proposed IDS outperforms the existing system which is due to the optimized selection of distributed watchdog nodes, security mechanisms which includes the combination of active and passive monitoring techniques along with the influence of routing protocols. Thus, the proposed system reduces the influence of attackers present in the network which in turn improves the above mentioned performance metrics.

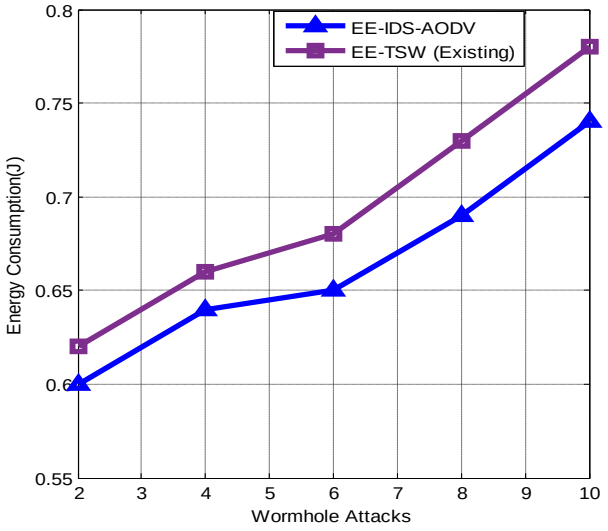


Figure 4.8 Energy consumption versus Attacks

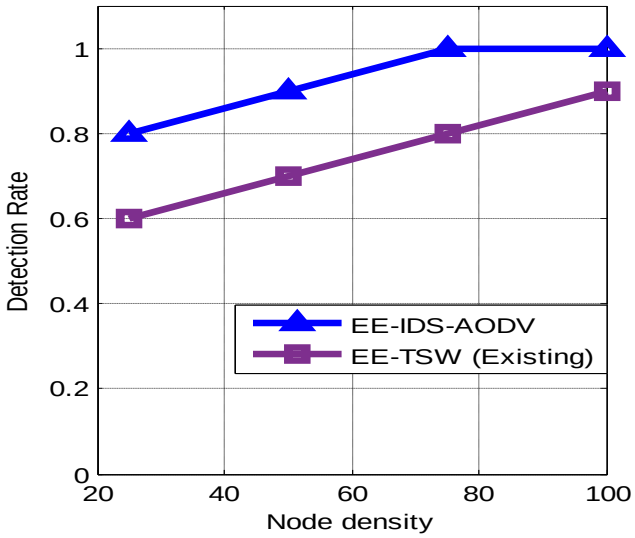


Figure 4.9 Detection rate versus Node density

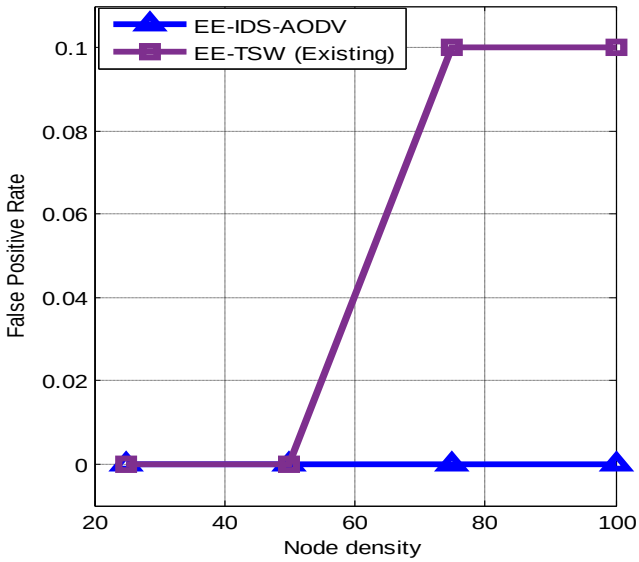


Figure 4.10 False Positive Rate versus Node density

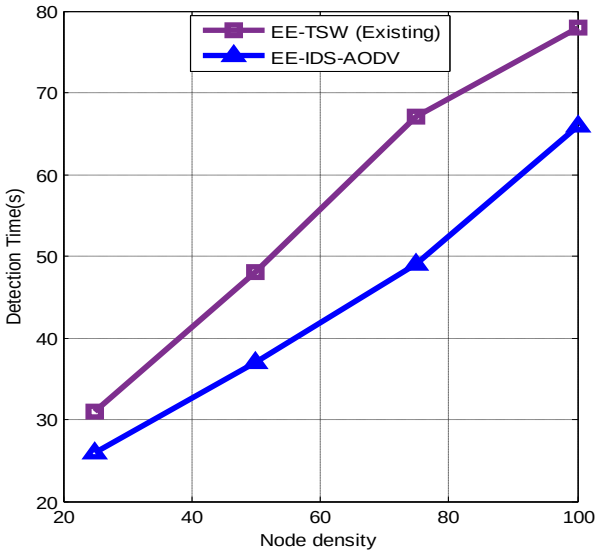


Figure 4.11 Detection time versus Node density

The significant performance metrics of IDS such as detection rate, false positive rate and average detection time are illustrated from figure 4.9 to 4.11 respectively. The detection rate or true positive rate is shown in figure 4.8, which is measured by the ratio of intrusion instances detected by the system (True Positive) to the total number of intrusion instances present in the test set. It is observed through the figure 4.9 that the detection rate is increased for increased node density for existing and proposed IDS. The FPR of proposed IDS shown in figure 4.10 refers to normal events predicted as attackers. Similarly, the detection time of proposed system

consume less time (approximately 65 seconds) than that of existing system for detection of five pairs of wormhole attack as shown in fig. 4.11. Further, in terms of IDS metrics, the proposed system achieves 24 % of enhancement in detection rate, 20% of reduction in detection time than that of existing system. It is depicted through the figure 4.10 that the proposed system achieves 0% FPR. Since the proposed system detects the wormhole attacker nodes very earlier than existing system, the detection time taken by the proposed system is very lesser than the existing system,. After detecting the attacker nodes, the connection between the attacker nodes and the network is disconnected quickly, this in turn reduces the overall effect of attacker nodes in the network. Hence, the performance metrics of proposed system is enhanced.

4.6. SUMMARY

In this chapter, EE-IDS with AODV is developed for Zigbee based WSN to detect the wormhole attack. The performance of ZigBee based WSN using proposed EE-IDS-AODV such as packet delivery ratio, average end-to-end delay and energy consumption are determined and compared with EE-TSW. The proposed EE-IDS-AODV is also evaluated and compared with existing system in terms of metrics such as detection rate, false positive rate and detection time. Thus, the proposed system reduces the influence of attacker nodes in the network and enhances the performance metrics compared to that of the existing system.

CHAPTER-5

ENERGY EFFICIENT INTRUSION DETECTION SYSTEM WITH STR ROUTING PROTOCOL

5.1. INTRODUCTION

In this chapter, the Energy Efficient Intrusion Detection System (EE- IDS) with Shortcut Routing Protocol (STR) developed for ZigBee based Wireless Sensor Networks through simulation in order to detect the wormhole attacks is discussed. Further, the performance metrics such as Packet Delivery Ratio (PDR), End-to-End Delay, and Energy Consumption are determined and compared with that of existing Energy Efficient Trust system for wormhole detection (EE-TSW). Furthermore, the metrics such as detection rate, FPR and detection time of proposed EE-IDS are examined to evaluate the efficiency of the proposed system EE-IDS-STR.

5.2. SHORTCUT TREE ROUTING PROTOCOL

The STR algorithm [70- 71] is developed to solve the detouring path problem of Zigbee Tree Routing [72] (ZTR) by using 1-hop neighbor information. The ZTR requires the highest hop distance since it has a detouring path problem due to the packets follows a tree topology. The STR algorithm is basically ZTR, but chooses one of neighbour nodes as the next hop node when the remaining tree hops to the destination is reduced. The objective of STR is to compute the remaining hops from an arbitrary source to a destination by using hierarchical addressing scheme in ZigBee.

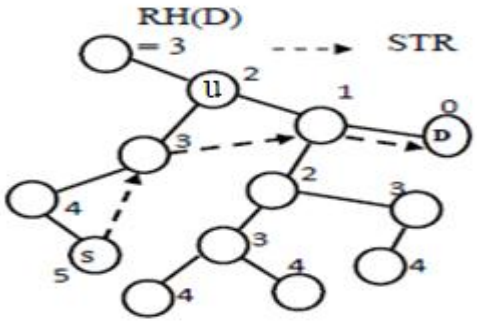


Figure 5.1 Shortcut Tree Routing [70]

Figure 5.1 illustrates the example of STR, where RH(D) is represented as the remaining hops to the destination from a received node u. S and D indicates as sender and destination node in the network. When the source node sends a packet to the destination node, a sender node (S) determines the next hop node in STR; thus, a routing path cannot be changed even link failure or traffic congestion is occurred. Generally, packet transmission between source and destination in STR is done by selecting the next hop neighbor node, which has the minimum remaining hop to the destination. By using next hop neighbor node selection instead of the tree link, STR reduces the maximum hop distance to transmit a packet to the destination. Thus, STR achieves lesser end-to-end delay and higher PDR when compared to that of ZTR protocol. In case, if there is no next hop neighbor node to decrease the remaining hops to the destination, STR will choose the parent or one of the children node as the next hop node as ZTR.

5.3. PROPOSED EE-IDS-STR

The functional flow diagram of EE-IDS-STR shown in the figure 5.2 is similar to that of EE-IDS-AODV described in the previous chapter except the routing protocol. In EE-IDS-STR, the short cut tree routing protocol is appended along with security mechanism EE-IDS to analyze the performance of ZigBee wireless sensor network in the presence of wormhole attack.

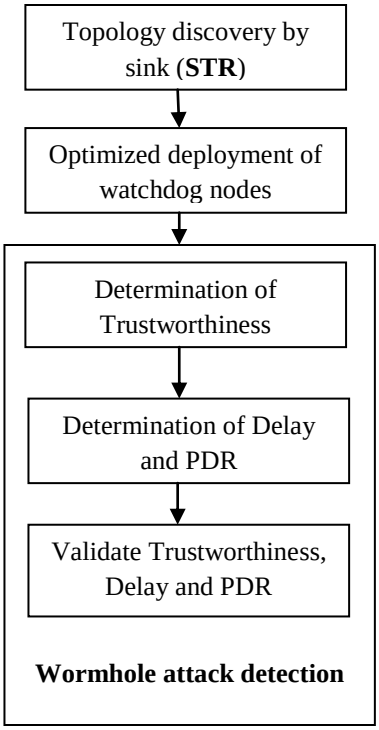


Figure 5.2 Functional flow diagram of EE-IDS-STR

Here also, the functional flow diagram of EE-IDS-STR comprises of three main phases. They are topology discovery, optimized deployment of watchdog nodes and detection of wormhole attack. In topology discovery phase, a routing protocol known as STR is used for discovering network topology. Following the topology discovery phase, optimized deployment of watchdog nodes and detection of wormhole attacks are done, which is clearly explained in the previous chapter. The wormhole attack detection is also based on finding of the three factors such as trustworthiness of the nodes, the abnormal deviation in the end to end delay and PDR. which is explained in the chapter 4.

5.4. SIMULATION RESULTS AND DISCUSSION

The effectiveness of proposed approach is examined in terms of packet delivery ratio, average end-to-end delay, energy consumption, detection rate, false positive rate as well as average detection time by varying number of wormhole attacker and node density. Finally, the simulation results of the proposed system namely EE-IDS is compared with the existing EE-TSW. The parameters used for this simulation are shown in the table-5.1. Figure 5.3 depicts the Zigbee network scenario with wormhole attacks. The Zigbee network scenario consists of 100 numbers of nodes deployed randomly over the terrain area of size 100 x 100 m^2. Nodes circled with red color indicate the wormhole attacker nodes deployed randomly into the ZigBee networks.

Table 5.1 Simulation Parameters for EE-IDS-STR

No. of Nodes	25, 50, 75, 100
MAC	IEEE 802.15.4
Routing Protocol	STR
Area	100 X 100 m^2,
Attackers (Wormhole attack)	5 Pairs of attackers
Traffic Source	Poisson
Simulation Time	100 sec
Initial Energy of node	1 Joule
Propagation model	Two Ray Ground

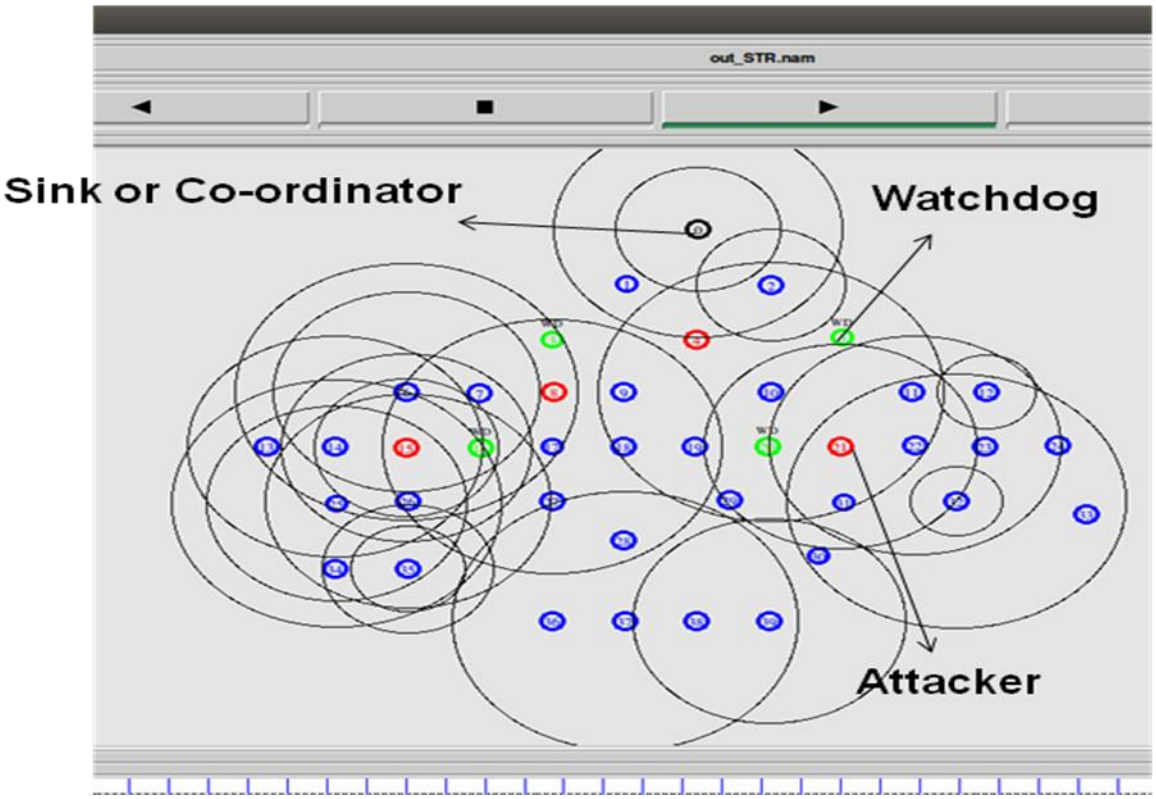


Figure 5.3 Zigbee WSN scenario with Wormhole attacks

The green color nodes are watchdog nodes selected by the sink or coordinator based on the certain condition as explained in previous section. The parent node to all the nodes is a sink node indicated in black color and then normal nodes are indicated by blue color nodes which are illustrated in figure. 5.3.

The simulation results shown from the figure 5.4 to 5.6 depicts the packet delivery ratio, average end-to-end delay and energy consumption for various number of wormhole attacks. It is evident from the figure5.4 that PDR decreases for increased wormhole attacks, also it is inferred from the result that proposed IDS namely EE-IDS-STR shows better PDR than the existing EE-TSW by approximately 28%. Further, proposed EE-IDS-STR obtains improved performance in terms of reduced average end-to-end delay by approximately 8.8% which is illustrated through figure 5.5.

Furthermore, the proposed EE-IDS with STR achieves improved reduction in energy consumption than that of the existing EE-TSW by 10% as depicted in figure 5.6.

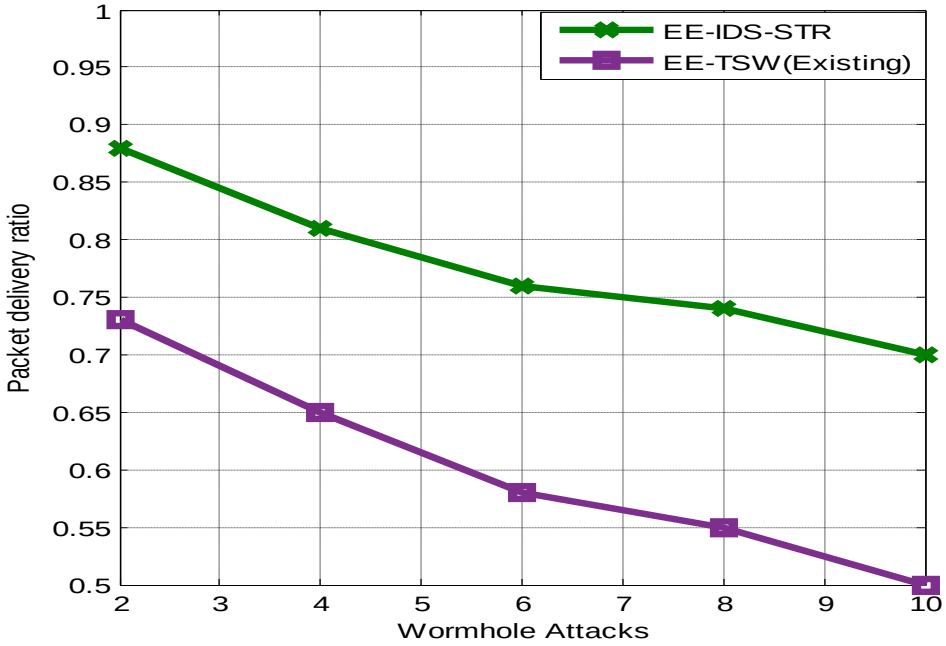


Figure 5.4 Packet delivery ratio Versus Attacks

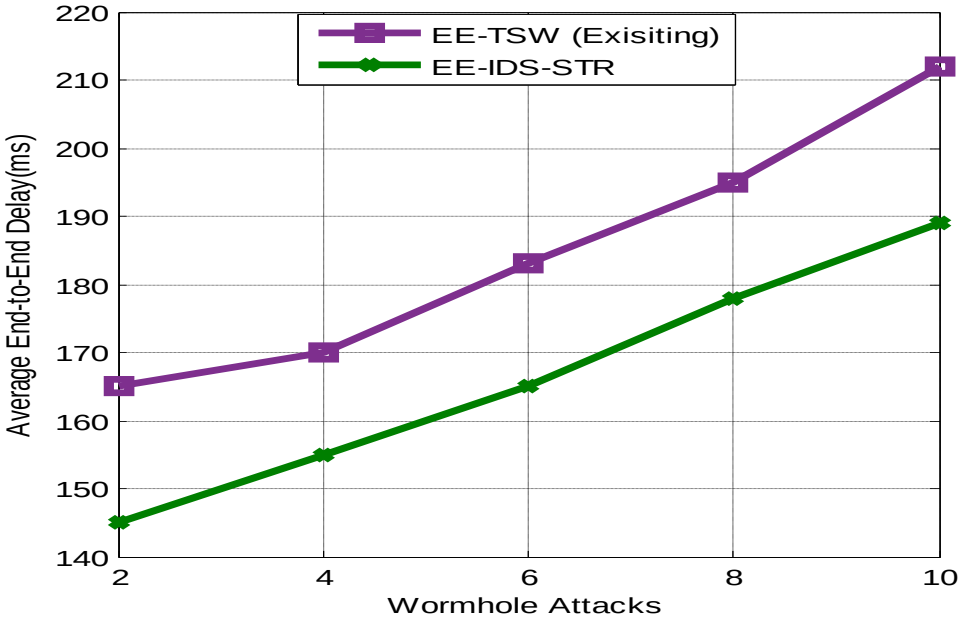


Figure 5.5 Avg. End-to-End Delay Versus Attacks

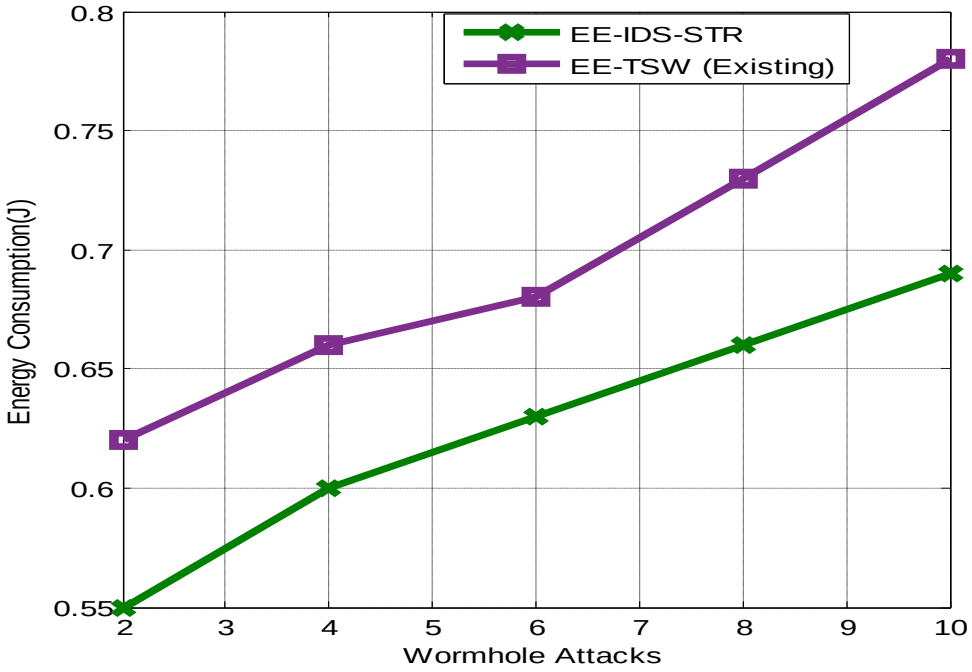


Figure 5.6 Energy consumption Versus Attacks

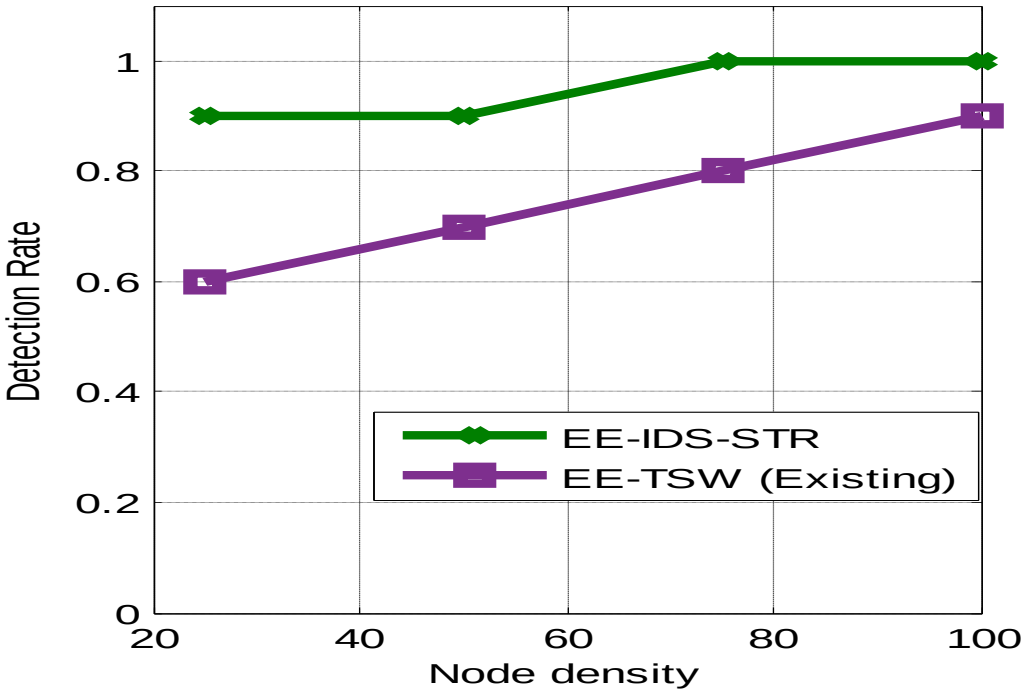


Figure 5.7 Detection rate Versus Node density

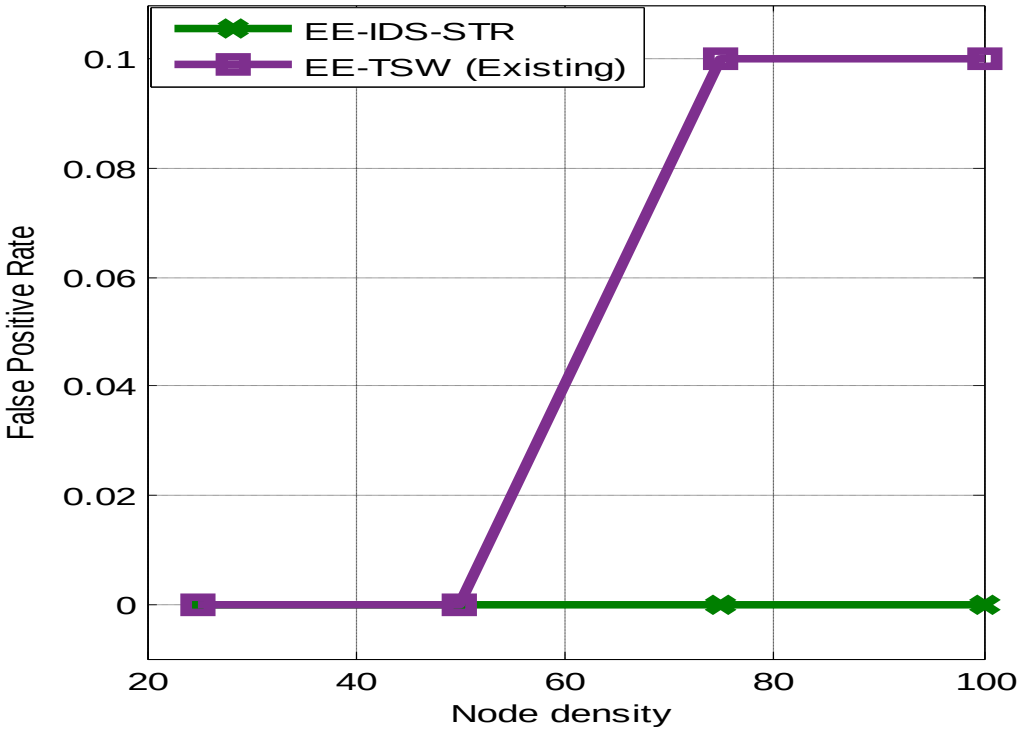


Figure 5.8 False Positive Rate Versus Node density

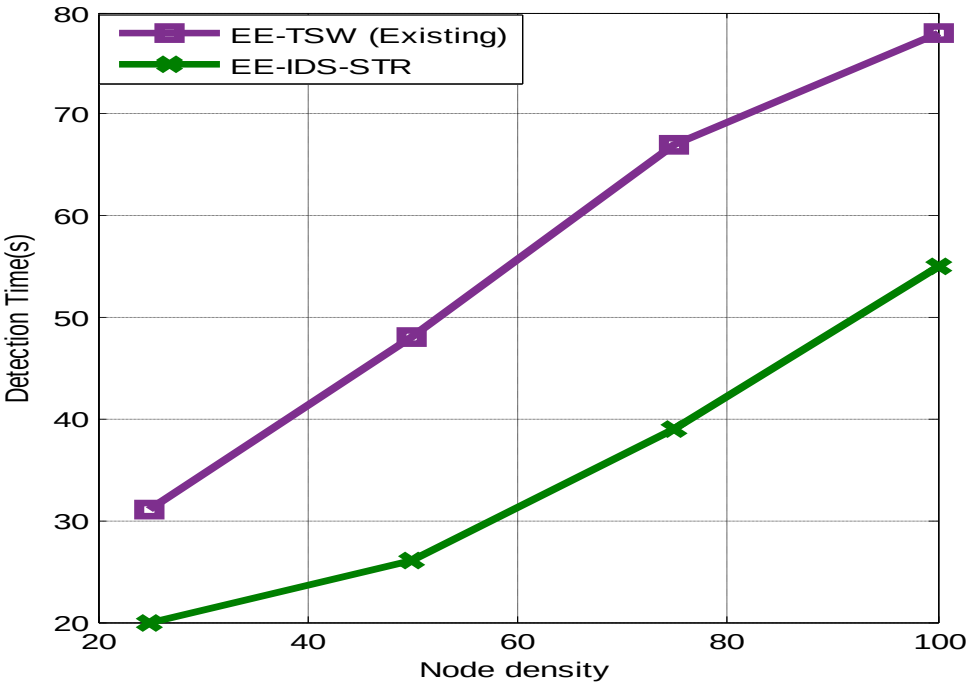


Figure 5.9 Detection time Versus Node density

The important performance metrics of IDS such as detection rate, false positive rate and average detection time are illustrated from figure5.7 to 5.9 respectively. The detection rate or true positive rate is shown in figure 5.7. It is inferred from the figure 5.7 that the detection rate increases with respect to increased node density for existing and proposed IDS. The FPR of proposed IDS is depicted in figure 5.8. Further, the detection time of proposed system for detection of wormhole attack is lesser than that of the existing systems shown in figure 5.9. The enhanced performance metrics is achieved through the EE-IDS-STR is due to the reduced effect of attackers and isolation of the malicious nodes from the network that is achieved with the aid of watchdog nodes and inherent features of STR protocol used in the EE-IDS-STR.

From the overall simulated results illustrated from figure 5.4 to 5.9, it is inferred that proposed EE-IDS-STR outperforms the EE-TSW by 28% improvement in terms of packet delivery ratio, 8.8% reduction in terms of end-to-end delay and 10% reduction in terms of energy consumption with respect to wormhole attacks. Further in terms of IDS metrics, the proposed system achieves 28 % of enhancement in detection rate,38% of reduction in detection time than that of existing system and EE-IDS-STR achieves 0% False Positive Rate (FPR).

5.5. SUMMARY

In this module, EE-IDS with STR is developed for Zigbee based WSN under wormhole attack. The performance of Zigbee based WSN using proposed EE-IDS with STR such as packet delivery ratio, Avg. End-to-End delay and energy consumption are determined and compared with EE-TSW.The proposed EE-IDS-STR is also examined and compared with existing system in terms of metrics such as detection rate, false positive rate and detection time. It is inferred through the overall simulation results that EE-IDS-STR outperforms the existing system in terms of above mentioned metrics.

CHAPTER-6

ENERGY EFFICIENT INTRUSION DETECTION SYSTEM WITH OSTR ROUTING PROTOCOL

6.1. INTRODUCTION

To enhance the performance of ZigBee wireless sensor network still further against wormhole attack, Energy Efficient Intrusion Detection System (EE- IDS) with Opportunistic Shortcut Routing Protocol (OSTR) is developed through simulation for ZigBee based Wireless Sensor Networks which is discussed in this chapter. Further, the performance metrics such as Packet Delivery Ratio (PDR), End-to-End Delay, and Energy Consumption are determined and compared with that of existing Energy Efficient Trust system (EE-TSW). In addition to this, the metrics such as detection rate, FPR and detection time of proposed EE-IDS are also examined to evaluate the efficiency of the proposed system EE-IDS-OSTR.

6.2. OPPORTUNISTIC SHORTCUT TREE ROUTING PROTOCOL

Opportunistic Routing [73-76] (OR) and Shortcut Tree Routing (STR) are integrated to obtain the OSTR [72] to resolve the issues of ZTR and STR. In fact, as STR, OSTR also uses a tree routing cost as a routing metric and finds out the remaining hops to the destination with the help of ZigBee hierarchical addressing scheme. In any case, a sender node just broadcasts a message rather than assigning a next hop node and receiver nodes contend to forward a message with requirement of the remaining hops. Hence, it is planned all together that the sensor node nearest to the destination node among receiver nodes put forwards a message. In addition to this, the selection of forwarder node and node prioritization are chosen in view of the one hop neighbor table and remaining hops with no unified or separate technique. In OSTR, there is no need of route discovery and routing table to transmit a message to the destination node because distance between sender and destination node can be determined by breaking down the ZigBee hierarchical structure.

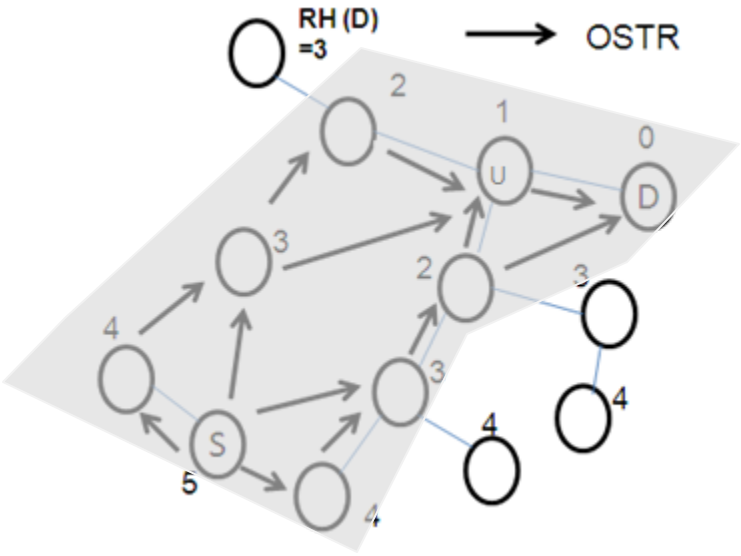


Figure 6.1 Opportunistic Shortcut Tree Routing [72]

Figure 6.1 demonstrates the OSTR, where RH(D) is signified as the remaining hops to the destination node from a received node U. In Figure 5.1 of the previous chapter, the subsequent hop node in both ZTR and STR is determined by a sender node; thus, a routing path cannot be altered even lossy communication link or traffic congestion is exist. Despite, what might be expected, the OSTR routing path in figure 6.1 can be changeable as per the communication link and condition of the traffic. In figure 6.1, the sensor nodes present within the gray area are forwarder nodes by considering a source node S to send a message to the destination D, and forwarders are chosen dynamically based on the sensor node having lesser number of hops to the destination and packet reception are the main concern of remaining hops to the destination. Because of active participation of neighbor nodes, OSTR enhances the reliability of packet delivery and competence of channel utilization through dynamic involvement of neighbor nodes.

Reducing the messages from the multiple forwarder candidates and decreasing the end-to-end latency between source nodes to the destination node are the most important goal of OSTR. In order to deal with this issue, OSTR has adapted overhearing and cancellation mechanism in view of the remaining hops to destination. Since the OSTR has acquired the benefits of STR and OR, the selection of forwarder node for determining routing path and

acquiring prior knowledge are not required. This approach makes resource constrained device to implement with the OSTR and offers efficient and reliable PDR services. And also, the OSTR reduces the end-to-end routing path by using Opportunistic Routing (OR) approach so that recipient node decides to forward a message or not.

6.3. PROPOSED EE-IDS-OSTR

The proposed system EE-IDS-OSTR functional flow diagram shown in the figure 6.2 is same as that of functional diagram of EE-IDS-STR explained in the previous chapter except the routing protocol. In EE-IDS-OSTR, the OSTR protocol is incorporating along with security mechanism EE-IDS to examine the performance of ZigBee wireless sensor network in the presence of attackers.

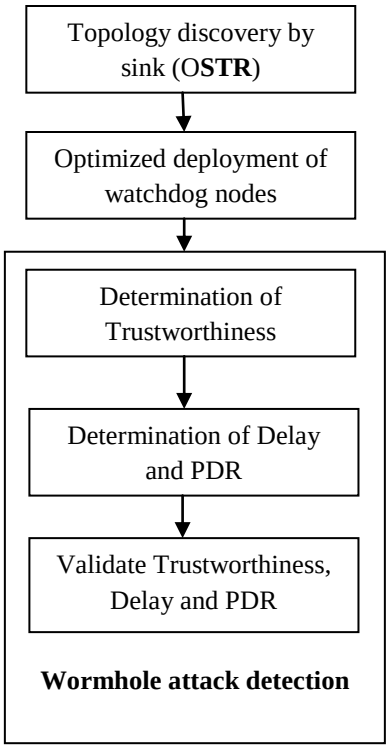


Figure 6.2 Functional flow diagram of EE-IDS-OSTR

The functional flow diagram of EE-IDS-OSTR consists of three main phases. They are topology discovery, optimized deployment of watchdog nodes and detection of wormhole attack which are described in the chapter-3. In topology discovery phase, a routing protocol known as OSTR is used for discovering the network topology, which is conducted by the sink node so that

the routing path from each node to the sink is stored in the respective nodes. Following the topology discovery phase, optimized deployment of watchdog nodes and detection of wormhole attacks are done, which is clearly described in the chapter-3.

6.4. SIMULATION RESULTS AND DISCUSSION

The effectiveness of the proposed approach EE-IDS-OSTR is examined through the performance metrics in terms of packet delivery ratio, average end-to-end delay, energy consumption, detection rate, false positive rate as well as average detection time by varying number of wormhole attacker and node density. Finally, the simulation results of the proposed system namely EE-IDS is compared with the existing EE-TSW. The parameters used for this simulation are shown in the table-6.1. Figure 6.3 illustrates the ZigBee WSN scenario with wormhole attack. It consists of 100 number of nodes deployed randomly over the terrain area of size 100 x 100 m^2. The wormhole attacker nodes are deployed randomly into the networks which are indicated by nodes circled with red color.

Table 6.1 Simulation Parameters for EE-IDS-OSTR

No. of Nodes	25, 50, 75, 100
Area	100 X 100 m^2,
MAC	IEEE 802.15.4
Routing Protocol	OSTR
Simulation Time	100 sec
Traffic Source	Poisson
Attackers (Wormhole attack)	5 pairs of attacker
Initial energy of node	1 Joule
Propagation model	Two Ray Ground

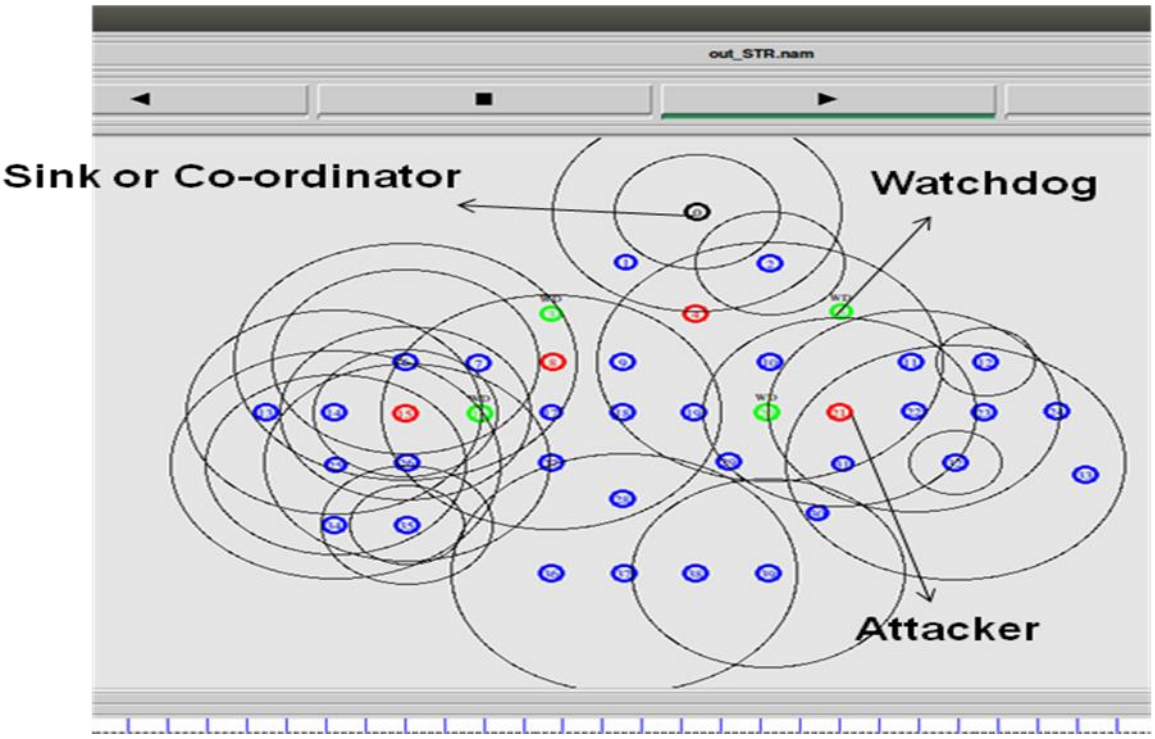


Figure 6.3 ZigBee WSN scenario with Wormhole attacks

The green color nodes are watchdog nodes selected by the sink or coordinator based on the certain condition as explained in previous section. The parent node to all the nodes is a sink node indicated in black color which is illustrated in figure 6.3. The simulation results shown from the figure 6.4 to 6.6 depicts the packet delivery ratio, average end-to-end delay and energy consumption with respect to number of wormhole attacks.

It is clear from the figure 6.4 that PDR decreases w.r.t increased wormhole attacks, also it is inferred from the result that proposed IDS namely EE-IDS-OSTR achieves better PDR than that of existing EE-TSW by approximately 35%. In figure 6.5, proposed EE-IDS-OSTR obtains the improved performance in terms of reduced average end-to-end delay by approximately 7%. Further, the proposed EE-IDS with OSTR also achieve improved reduction in energy consumption than that of the existing EE-TSW by 12.3% as depicted in figure 6.6.

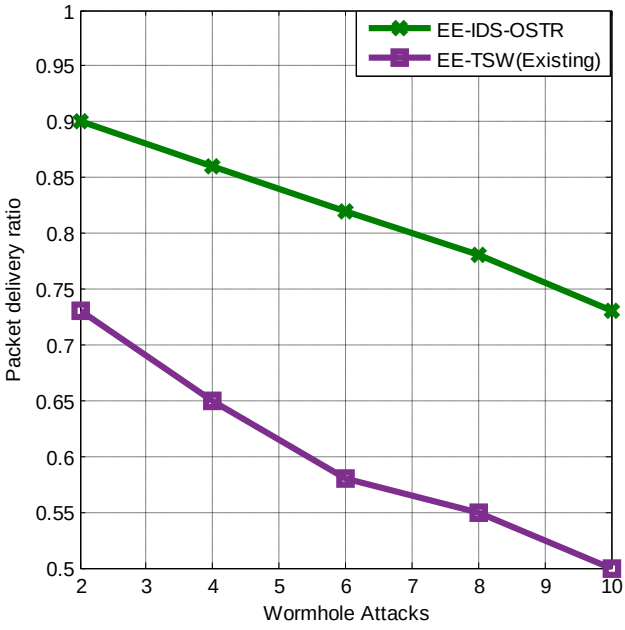


Figure 6.4.Packet delivery ratio Versus Attacks

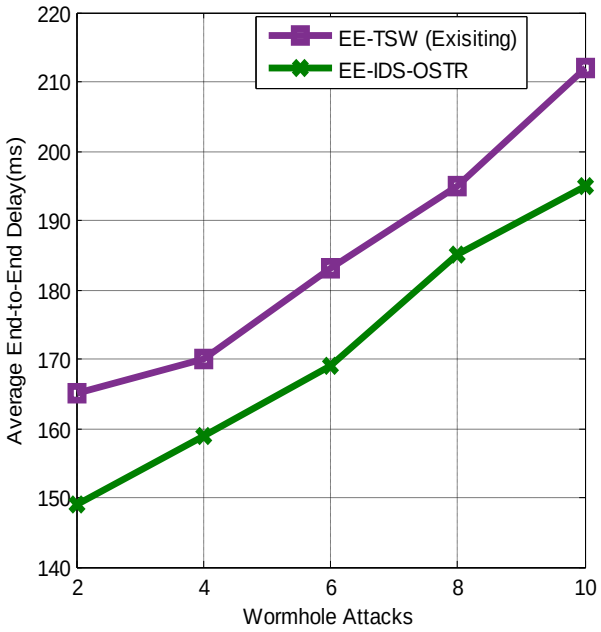


Figure 6.5. Avg. En d-to-End Delay Versus Attacks

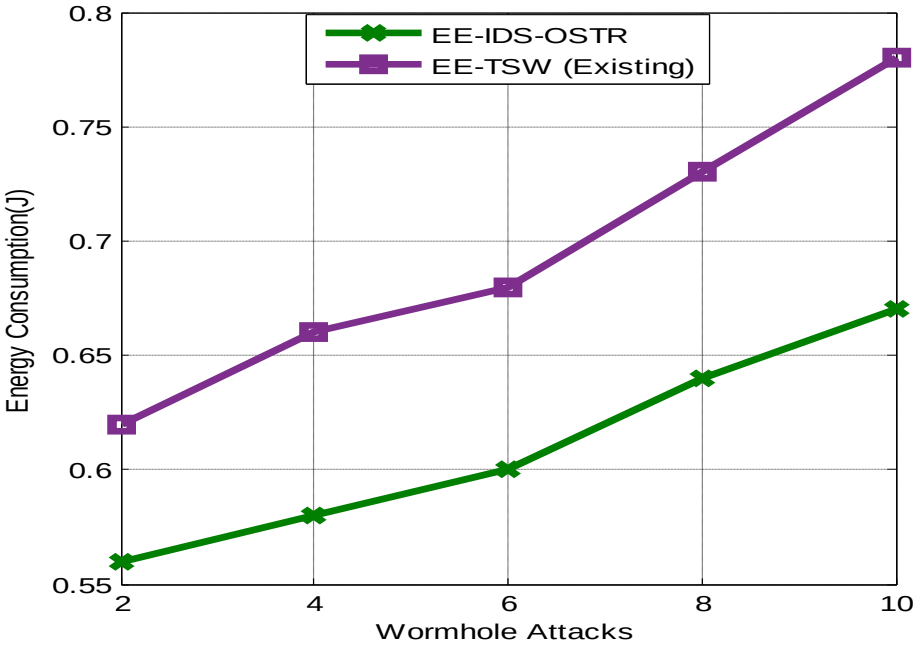


Figure 6.6 Energy consumption Versus Attacks

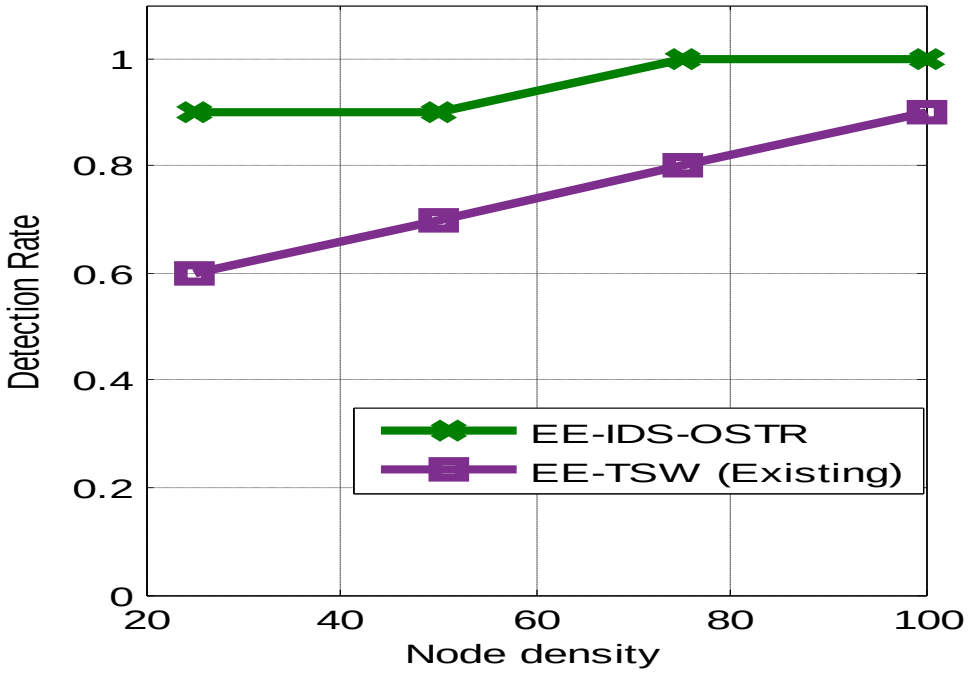


Figure 6.7 Detection rate versus Node density

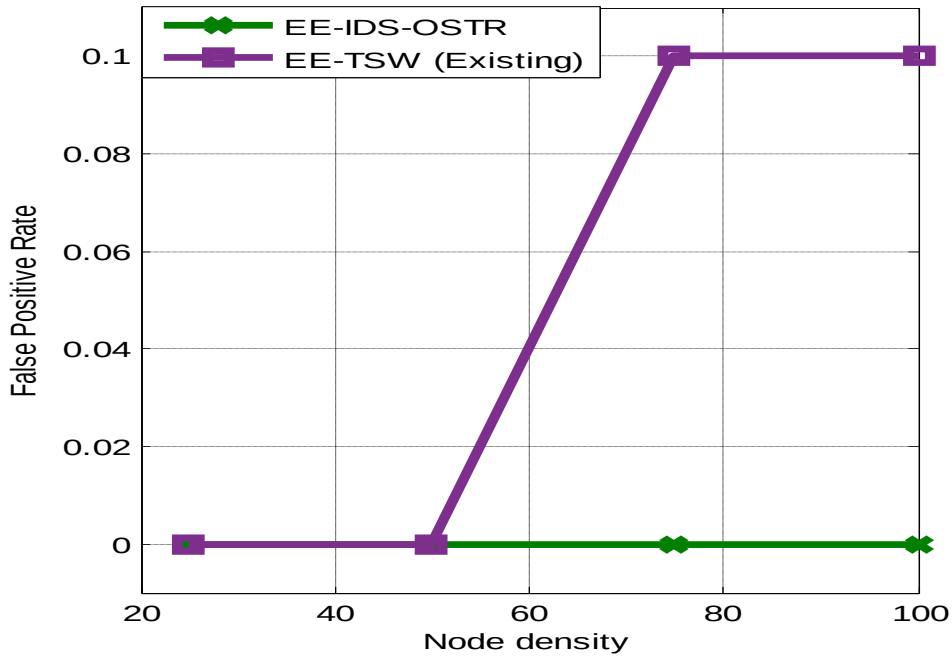


Figure 6.8 False Positive Rate Versus Node density

The significant performance metrics of IDS such as detection rate, false positive rate and average detection time are illustrated from fig. 6.7 to 6.9 respectively. It is observed through the

figure 6.7 that the detection rate increases with respect to increased node density for existing and proposed IDS with OSTR. It is noted through the figure 6.8 that proposed system provides 0% FPR. Further, the detection time shown in figure 6.9depicts that proposed system consume less time for detection of wormhole attack compared to that of existing system.

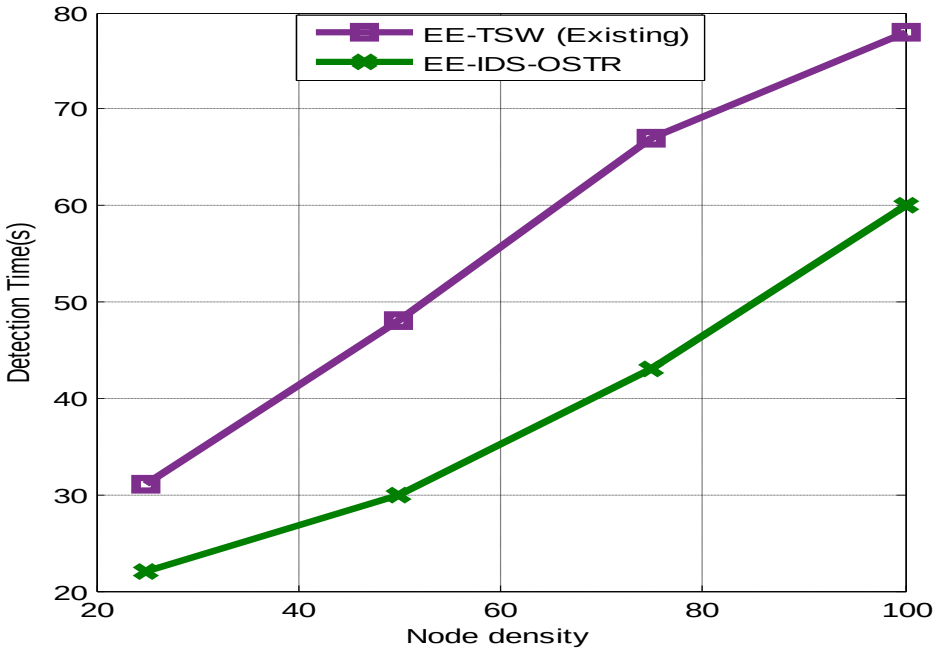


Figure 6.9 Detection time Versus Node density

From the overall simulated results illustrated from figure 6.4 to 6.9, it is inferred that proposed EE-IDS-OSTR outperforms the EE-TSW by 35% improvement in terms of packet delivery ratio, 9% reduction in terms of end-to-end delay and 12.3% reduction in terms of energy consumption w.r.t wormhole attacks. Further, in terms of IDS metrics , the proposed system achieves 28 % of enhancement in detection rate,32% of reduction in detection time compared to that of existing system and EE-IDS-OSTR also achieves 0% False Positive Rate (FPR). With the aid of energy efficient watchdog nodes, the performance metrics of the EE-IDS-OSTR is enhanced by reducing influence of attackers and preventing them from the network.

6.5. OVERALL COMPARISON OF PROPOSED IDS WITH EXISTING SYSTEM

This section illustrates the comparison of simulation results of proposed EE-IDS with that of existing EE-TSW. The simulation results shown from figure 6.10 to 6.12 depict the packet

delivery ratio, average end-to-end delay and energy consumption with respect to wormhole attacks.

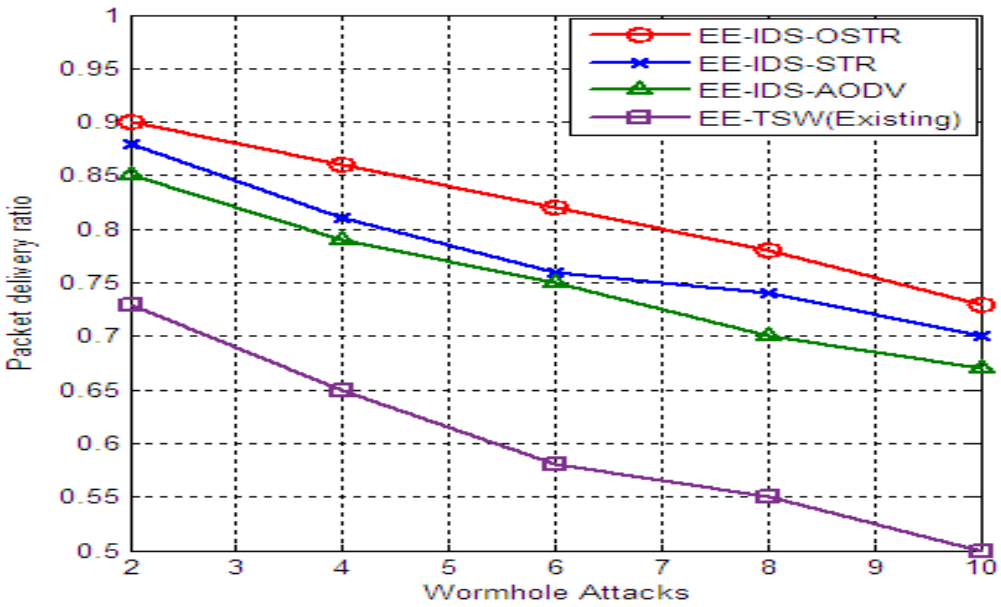


Figure 6.10 Packet delivery ratio Versus Attacks

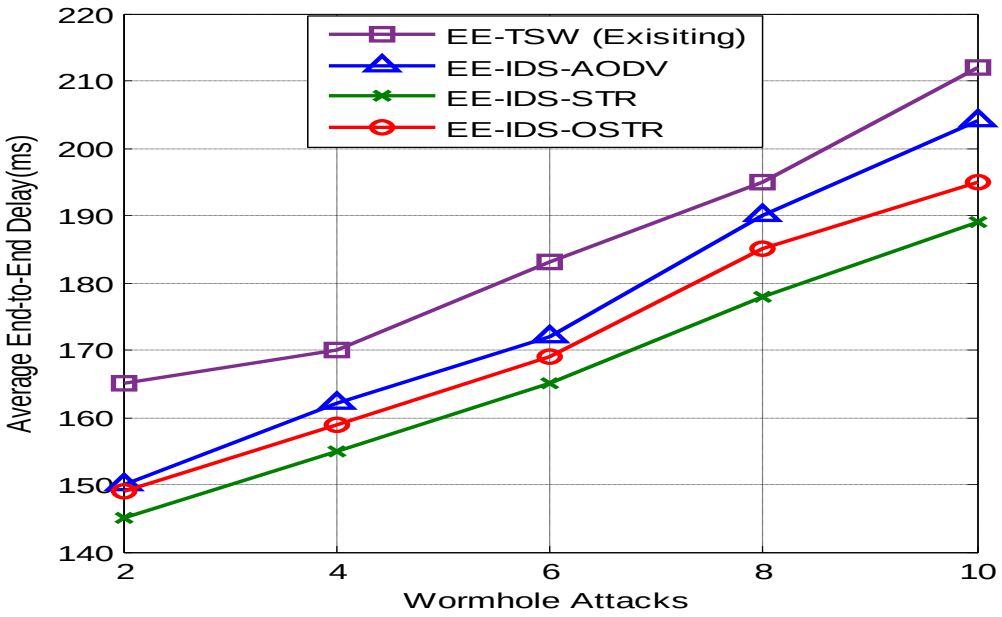


Figure 6.11 Average end-to-end delay Versus Attacks

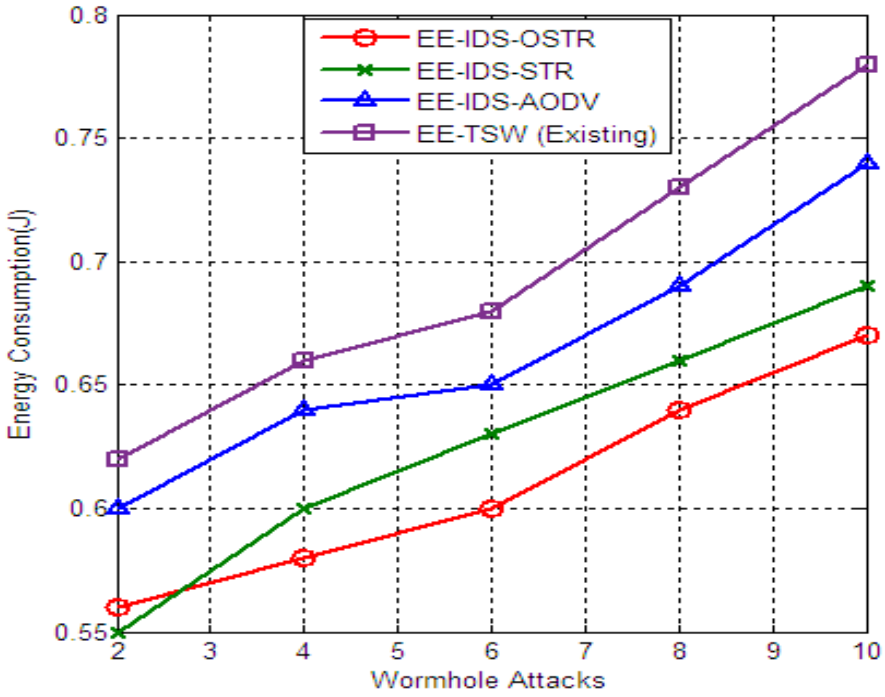


Figure 6.12 Energy consumption versus Attacks

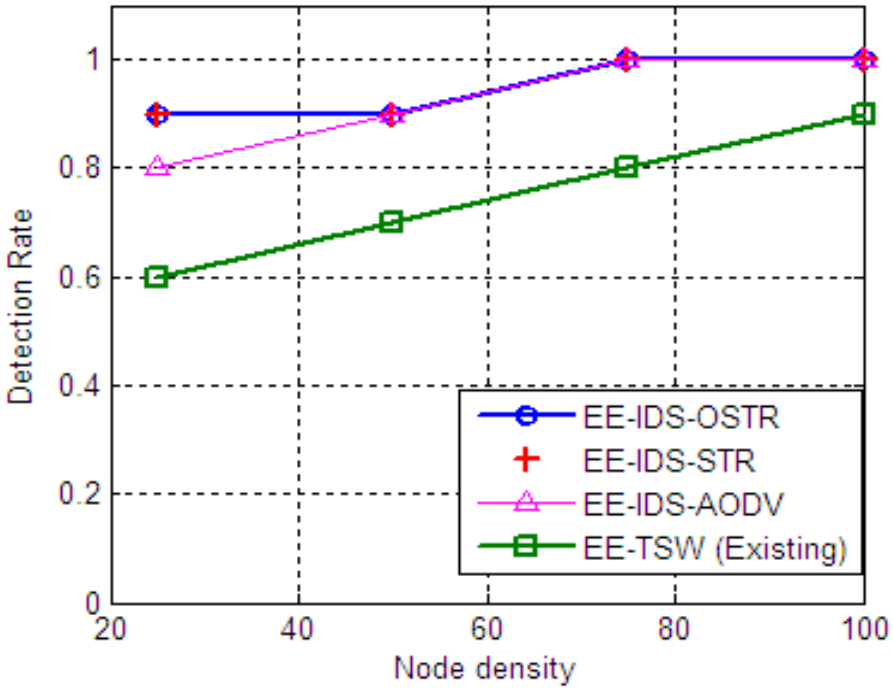


Figure 6.13 Detection Rate versus Node density

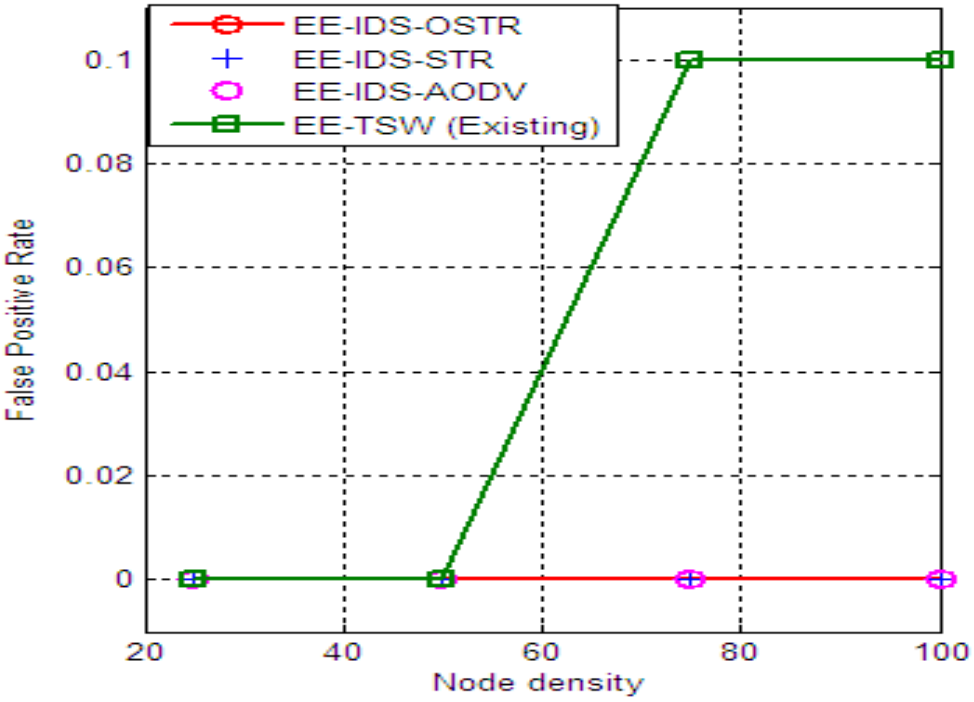


Figure 6.14. False Positive Rate Versus Node density

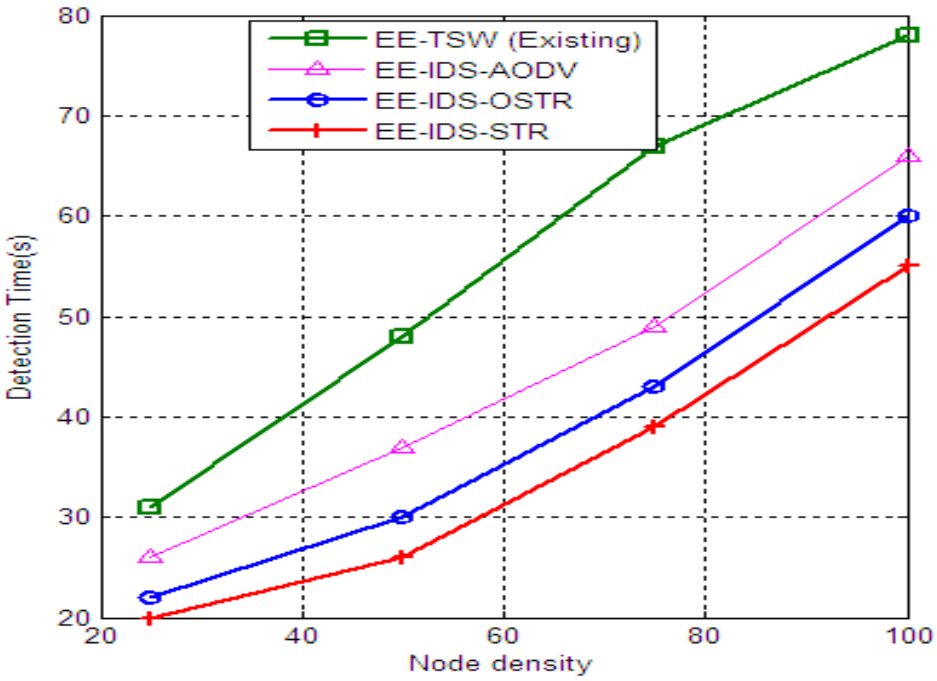


Figure 6.15 Detection Time versus Node density

It is observed through the overall simulation results illustrated from figure 6.10 to 6.15 that EE-TS-OSTR outperforms the EE-TS-AODV, EE-TS-STR and existing system in terms of performance metrics such as PDR, energy consumption, detection rate. This is due to the influence of proposed EE-IDS and the OSTR protocol. In OSTR protocol, packet delivery is high due to the reliable communication through diverse number of candidates which in turn reduces the energy consumption by sending the packets to destination via reliable path without retransmit the same packet. In case of STR, if the communication link between child to parent in the same branch is get broken, then there is no alternate path to establish the communication link to send the packets to the destination, which leads to packet retransmission via broken link repeatedly which in turn consume more power. The main drawback of the OSTR is longer delay when compare to that of STR which is due to hop delay that is used for prioritize the node for forwarding the packets. In terms of performance metrics such as average end-to-end delay and detection time, the proposed EE-IDS-STR achieves better performance than that of other systems.

6.6. SUMMARY

In this module, EE-IDS with OSTR is developed for Zigbee based WSN under wormhole attack. The performance of Zigbee based WSN using proposed EE-IDS with OSTR such as packet delivery ratio, average end-to-end delay and energy consumption are determined and compared with EE-TS.The proposed EE-IDS-OSTR is also evaluated and compared with existing system in terms of performance metrics such as detection rate, FPR and detection time. From the overall simulation results, it is noticed that the proposed EE-IDS-OSTR outperforms the existing system in terms of above mentioned performance metrics.

CHAPTER-7

CONCLUSION AND FUTURE SCOPE

7.1 CONCLUSION

This thesis is mainly centered on maximizing the node security and minimizing energy consumption throughout the ZigBee WSN under DDoS (Energy Exhaustion) and wormhole attack. It is done by developing the energy efficient intrusion detection mechanism through simulation to detect and prevent the DDoS and wormhole attacks in ZigBee WSN. The proposed systems developed for ZigBee WSN under DDoS and wormhole attack is tested by considering 100 numbers of sensor nodes deployed in a area of 100 x 100 square meters by varying the node density and attacker nodes. The significance of the proposed energy efficient intrusion detection systems is examined through the simulation in terms of network and IDS performance parameters.

- In module-1, EE-IDSEP is developed to enhance the security and minimize the energy consumption in the ZigBee WSN under DDoS attacks. The performance metrics such as PDR, average end-to-end delay and energy consumption are determined and analyzed through simulation. It is evident from the results that EE-IDSEP outperforms EE-TS by 12% improvement in terms of packet delivery ratio, 10% reduction in terms of packet drop and 15% reduction in terms of energy consumption. The significance metrics of IDS such as detection rate, FPR and detection time examined through simulation proves that the proposed system EE-IDSEP achieves approximately 33.3 % enhancement in detection rate and 22.5 % of reduction in detection time compared to that of existing system and EE-IDSEP achieves 4.6 % in FPR.

- The proposed security mechanism namely EE-IDS-AODV for detection of wormhole attack in ZigBee WSN is dealt in module 2. In this module, the above-mentioned performance metrics of ZigBee WSN is studied through simulation by using EE-IDS-AODV mechanism. It is inferred through the results that EE-IDS-AODV achieves better performance than the existing EE-TSW by approximately 23% improvement in terms of PDR and 5.4% reduction in average end-to-end delay and 4.3% reduction in energy consumption. The proposed system also achieves an enhancement in the detection rate by

approximately 24% and reduction in the detection time by 20% than that of existing method and proposed system also provides 0% FPR.

- In third and fourth module, the proposed systems EE-IDS-STR and EE-IDS-OSTR are developed for the detection of wormhole attacks in ZigBee WSN. The above mentioned network performance metrics are analyzed through simulation by using the developed EE -IDS-STR and EE-IDS-OSTR. It is depicted through the simulation results that the proposed IDS namely EE-IDS-STR and EE-IDS-OSTR obtain better performance than the existing EE-TSW by approximately 28% and 35% improvement in terms of PDR, 8.8% and 7% reduction in average end-to-end delay and reduction in energy consumption by approximately 10% and 12.3% respectively. It is also observed from the results that proposed EE-IDS-STR and EE-IDS-OSTR achieves 28% enhancement in detection rate and approximately of 38% and 32% reduction in detection time respectively with 0% FPR for both proposed systems.

- Hence, ,it is concluded that, w.r.t DDoS attacks, the proposed system EE-IDSEP outperforms the existing system EE-TS in terms of the above mentioned performance metrics. Further, in case of wormhole attack, the proposed EE-IDS with OSTR protocol achieves overall improvised performance in terms of PDR, energy consumption, detection rate and FPR compared to that of EE-IDS- STR, EE-IDS-AODV and existing EE-TSW. Finally, it is found through the investigations that the proposed security mechanisms are well suited for ZigBee WSN to maintain better security with optimal energy consumption with the certain limitations of the least computational overhead.

7.2 SCOPE OF FUTURE WORK

This present research work can be upgraded to the next level of research by incorporating the following factors.

- In future, the performance of proposed EE-IDS for ZigBee WSN can also be analyzed by incorporating DOSTR in proposed EE-IDS

- It is also better to study the network performance of the proposed IDS system , in future by considering more than 100 numbers of nodes with varying parameters such as deployment area of node , variable bit rate traffic and more number of attackers
- The work can be extended by incorporating other approaches like game theory or machine learning model in the proposed system to detect unknown attacks.
- The work can be extended further by considering the tradeoff mechanism between the energy and memory storage to make the system well efficient for resource-constrained networks.
- The work can be still extended by appending mobility models to keep the system used for dynamic applications.

REFERENCES

[1]. Akyildiz, I.F., Weilian, Su.,Sankarasubramaniam, Y. and Cayirci, E.,"A survey on sensor networks", *IEEE Transactions Communications,* Vol.40, No.8, pp.102 -144, 2002.

[2]. Werner-Allen. G, Lorincz. K, Welsh. M, Marcillo.O, Johnson. J, Ruiz. M and Lees. J, "Deploying a wireless sensor network on an active, volcano", *IEEE Transactions on Internet Computing*, Vol.10, No.2**,** pp.18–25, 2006.

[3]. ZigBee Specification - Document 053474r17, *ZigBee Alliance*, 2007. http://www.zigbee.org/.

[4]. Paolo Baronti , Prashant Pillai , Vince W.C. Chook , Stefano Chessa ,Alberto Gotta, Y. Fun Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communications, Elsevier*, Vol.30, No.7,pp.1655-1695, December, 2007.

[5]. *802.15.4-2003 Standard, IEEE Computer Society*, 2003, ISBN (Print): 0-7381-3686-7 SH95127. http://www.ieee802.org/15/pub/TG4.html.

[6]. NIST.FIPS, *PUB 197: The AES standard*, 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[7]. FIPS, *PUB 46-2: Data Encryption Standard*. 1993 2008-01-23 http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[8]. Menezes, Oorschot, and Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.

[9]. Koblitz, " Elliptic curve cryptosystems", *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.

[10]. Shannon, "Communication Theory of Secrecy Systems", *Bell Systems Technical Journal*, pp. 656-715, 1949.

[11]. X. Du and H.H. Chen, "Security in wireless sensor networks", *IEEE Wireless Communications*, Vol.15, No.4, pp.60–66, 2008.

[12]. AbrorAbduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai-Choong Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", *IEEE Communications Surveys & Tutorials*, Third Quarter, Vol. 15, No. 3, pp. 1223-1237, 2013.

[13]. Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", *International Journal of Distributed Sensor Networks*,pp.102 -144, 2013.

[14]. Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", *IEEE Communications Surveys & Tutorials*, Vol. 16, No. 1,pp. 266-282, First Quarter 2014.

[15]. Amudhavel J et al., "A Survey on Intrusion Detection System: State of the Art Review", *Indian Journal of Science and Technology,* Vol. 9, No. 11, pp.1-9, March 2016.

[16]. IoannisKrontiris, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side", *Proceedings of the IEEE International Conference on Wireless and Mobile Computing,* France, pp. 526-531, Oct. 2008.

[17]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks", *IEEE Journal on selected areas in communications,* Vol. 24, No. 2, pp.370 – 380, February 2006.

[18]. Hu Y.C, Perrig A and Johnson B, "Packet leashes: a defense against wormhole attacks in wireless networks", *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications,* USA, pp. 1976-86, April 2003.

[19]. Capkun S, Buttyn L and Hubaux JP, " SECTOR: Secure tracking of node encounters in multi-hop wireless networks", *Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks* , USA, pp. 1-12, October 2003.

[20]. Hu L and Evans D, "Using directional antennas to prevent wormhole attacks", *Network and Distributed System Security Symposium* , California, USA, pp. 1-11, February 2004.

[21]. L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", *Proceedings of the IEEE Wireless Communications and Networking Conference,* USA, Vol. 2, pp. 1193 – 1199, March 2005.

[22]. Khalil I, Bagchi S, and Shroff NB, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", *Proceedings of the International Conference on Dependable Systems and Networks*, Japan, pp.612-621, July 2005.

[23]. N. Song, L.Qian, and X. Li, "Wormhole attack detection in wireless ad-hoc networks: A statistical analysis approach," *Proceedings of the IEEE International Parallel and Distributed Processing Systems*, USA, Vol. 4, pp. 2106 – 2111, March 2005.

[24]. L. Buttyan, L. Dora and I. Vajda, "Statistical wormhole detection in sensor networks," *Proceedings of the Springer European Workshop on Security in Ad-hoc and Sensor Networks (ESAS 2005), Lecture Notes in Computer Science,* Vol. 3813, pp. 128-141, 2005.

[25]. Wood AD, Fang L, Stankovic JA, He T, "SIGF: a family of configurable, secure routing protocols for wireless sensor networks", *Proceedings of the 4th ACM Workshop on Security of Adhoc and Sensor networks,* Alexandria, Virginia, USA, pp.35-48, 2006.

[26]. Wang J, Yang G, Chen S, Sun Y, "Secure LEACH routing protocol based on low-power cluster-head selection algorithm for wireless sensor networks", *Proceedings of the International Symposium on Intelligent Signal Processing and Communication systems* . Xiamen, China, pp. 15127–15158, June 2007.

[27]. Pathan. AS, Hong C. "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor networks", *Springer Journal on Annals of Telecommunication,* Vol. 63, No. 9, pp. 529-541, October 2008.

[28]. Kumar S, Jena S, "SCMRP: secure cluster based multipath routing protocol for wireless sensor networks", *Proceedings of the 6thInternational Conference on Wireless Communication and Sensor networks,* Allahabad, India, pp.1–6, 2010.

[29]. Jiliang Zhou, "Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks" , *International Journal of Distributed Sensor Networks,* pp.1-15, March 2013.

[30]. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking,* Boston, Mass, USA, pp. 56–67, August 2000.

[31]. X.Wang, L. Yang, and K. Chen, "SDD: secure directed diffusion protocol for sensor networks", *Proceedings of the 1stEuropean Workshop,* Germany, pp. 205–214, August 2004.

[32]. B. Zhang and L. Chen, "An Improved Key Management of ZigBee Protocol", *Proceedings of the Third International Symposium on Intelligent Information Technology and Security Informatics. IEEE Computer Society,* China, pp. 416-418, April 2010.

[33]. S.Seshabhattar, P. Yenigalla, P. Krier, and D. Engels, "Hummingbird key establishment protocol for low-power ZigBee", *Proceedings of the IEEE Consumer Communications and Networking Conference* ,USA, pp. 447-451,May 2011.

[34]. Y.Kwon and H. Kim, "Efficient group key management of ZigBee network for home automation", *Proceedings of the IEEE International Conference on in Consumer Electronics,* USA, pp.378 – 379, March 2012.

[35]. K. Choi, M. Yun, K. Chae, and M. Kim, "An enhanced key management using ZigBee Pro for wireless sensor networks", *Proceedings of the IEEE International Conference on Information Networking* ,Indonesia, pp. 399-403, Feb 2012.

[36]. W. R. Pires , T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks", *Proceedings of 18th International Conference on In Parallel and Distributed Processing Symposium,* New Mexico, pp. 24, 2004.

[37]. A. Wood and J. Stankovic, "Denial of service in sensor networks", *IEEE Computer Magazine*, Vol. 35, No. 10, pp. 54–62, 2002

[38]. David. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", *IEEE Pervasive Computing*, Vol. 7, No. 1, pp. 74-81, 2008.

[39]. Radosveta Sokullu, Ilker Korkmazy, Orhan Dagdevirenz, Anelia Mitsevax, Neeli R. Prasad, "An Investigation on IEEE802.15.4 MAC Layer Attacks", *Proceedings of the 10th International Symposium on Wireless Personal Multimedia Communications* , pp.1-5, 2007.

[40]. Sang Shin Jung, Marco Valero, Anu Bourgeois, and Raheem Beyah, "Attacking Beacon-enabled 802.15.4 Networks", *Security and Privacy in Communication Networks*, *Springer*, Heidelberg, Germany, pp. 253-271, 2010.

[41]. Colin P. O'Flynn, "Message Denial and Alteration on IEEE 802.15.4 Low-Power Radio Networks," *Proceedings of the 4th IEEE International Conference on New Technologies, Mobility and Security* (NTMS), Paris, France, pp. 1-5, January 2011.

[42]. C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", *IEEE Transactions on Parallel Distribution Systems*, Vol. 23, No. 5, pp. 835–843, 2012.

[43]. Niko Vidgren, Keijo Haataja, Jose Luis Patino-Andres, Juan Jose Ramirez-Sanchis, PekkaToivanen, "Security Threats in Zigbee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned", *Proceedings of the 46th Hawaii International Conference on System Sciences*, *IEEE computer society*, Maui, Hawaii,pp. 5132 - 5138, March 2012.

[44]. K. Gill, S-H. Yang and W. Wang "Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems" , *IET Wireless Sensor System*, Vol. 2, no. 4, pp.361–368, Dec. 2012.

[45]. Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks", *IEEE Transactions on Mobile Computing*, Vol. 12, no.2 pp.1-15, feb. 2013.

[46]. Saman Taghavi Zargar, James Joshi and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *IEEE Communication Surveys & Tutorials*, Vol. 15, No. 4, pp. 2046 – 2069, Fourth Quarter, February 2013

[47]. C. Balarengadurai and Dr. S. Saraswathi, "Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network", *International Journal of Computer Science Issues*, Vol. 10, Issue 6, No. 1, pp. 293-301, November 2013.

[48]. Bernardo M. David, Beatriz Santana, Laerte Peotta, Marcelo D. Holtz and Rafael Timóteo de Sousa Jr, "A Context-Dependent Trust Model for the MAC Layer in LR-WPANs", *International Journal on Computer Science and Engineering*, Vol. 02, No. 09, pp. 3007-3016, 2010.

[49]. Anthony D. Wood, John A. Stankovic, and Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4- based Wireless Networks", *Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 60-69, June2007.

[50]. A.P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz and H.C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," *Proceedings of 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks* ,Montreal, Canada, pp.16-23, October 2005.

[51]. R. Roman, J. Zhou, and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks" , *Proceedings of the Consumer Communications and Networking Conference*, Las Vegas, USA, pp. 640-644, 2006.

[52]. S. Mati , Giuli T, Lai K, Baker M, "Mitigating routing misbehavior in mobile ad hoc networks" *Proceedings of the 6th ACM International Conference on Mobile Computing and Networking*, Vol. 6, No. 11, pp 255-265, August 2000

[53]. I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Canada, pp. 253-259, October 2005.

[54]. V. Bhuse, A. Gupta, "Anomaly intrusion detection in wireless sensor network", *Journal of High Speed Networks*, Vol.15, No.1, pp 33-51, Jan 2006

[55]. Y.Zhenwei, J.J.P.Tsai, "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks," *In IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing* (SUTC'08), Taichung, Taiwan, pp. 272–279, June 2008

[56]. Chong Eik Loo, Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami. "Intrusion Detection for Routing Attacks in Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2, No. 4, pp. 313 – 332, December 2006.

[57]. I. Krontiris, T. Dimitriou, and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," *Proceedings of the 13th European Wireless Conference*, Paris, France, 2007.

[58]. Tran Hoang Hai, Faraz Khan, and Eui-Nam Huh, "Hybrid Intrusion Detection System for Wireless Sensor Network", *Proceedings of the International Conference on Computational Science and its Applications", Lecture Notes in Computer Science,* Berlin, Germany , Vol. 4706, pp. 383–396, , 2007.

[59]. A. Stetsko, L. Folkman and V. Matyáš, "Neighbor-based intrusion detection for wireless sensor networks", *Proceedings of the 6th International Conference on Wireless and Mobile Communications,* Valencia, Spain, pp. 420-425, 2010.

[60]. F. Nait-Abdesselam, B. Bensaou, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", *Security in Mobile Ad Hoc and Sensor Networks- IEEE Communication Magazine*, Vol.46, No.4, pp. 127 - 133, 2008.

[61]. Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, FuxiangGao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis," *Proceedings of WASE International Conference on Information Engineering*, Hebei, China, pp. 251-254, 2010.

[62]. Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, and Xiangke Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks," *IEEE/ACM Transactions on Networking,* Vol. 19, No. 6, pp. 1787-1796, December 2011

[63]. A.Forootaninia1 and M.B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique Based On Power-Aware Hierarchical Design For IDS In Wireless Sensor Networks," *International Journal of Network Security &its Applications*, Vol. 4, No. 4,pp. 161-178, July 2012.

[64]. Youngho Cho and Gang Qu and Yuanming Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks", *IEEE Computer Society on Security and Privacy Workshops*, pp. 134-141, 2012.

[65]. YanzhiRen et al., "Detecting Wormhole Attacks in Delay-Tolerant Networks [Security and Privacy in Emerging Wireless Networks]", *IEEE Wireless communications,* Vol. 17, No. 5, pp: 36-42, October 2010.

[66]. Peng Zhou, Siwei Jiang, AthiraiIrissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Te., "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs", *IEEE Transactions on Information Forensics and Security,* Vol.10, No.3, pp.613-625, March 2015.

[67]. C. Perkins, E. Belding-Royer, and S. Das, "RFC 3561: Ad-hoc on-demand distance vector (AODV) routing," July 2003.

[68]. Peng Hu, Zude Zhou, Quan Liu, and Fangmin Li, "The HMM-based modeling for the energy level prediction in wireless sensor networks", *Proceedings of the Second IEEE Conference on Industrial Electronics and Applications,* Harbin, China, pp. 2253 – 2258, May-2007.

[69]. Lawrence rabiner "A tutorial on hidden markov models and selected applications in speech recognition", *IEEE Journals & Magazines*, Vol. 77, No. 2, pp- 257 – 286, Feb 1989.

[70]. Taehong Kim, Daeyoung Kim*et al*, "Shortcut Tree Routing in ZigBee Networks," *Proceedings of 2nd International Symposium on Wireless Pervasive Computing,* San Juan, Puerto Rico, pp. 42-47, February 2007.

[71]. T. Kim, S. Hoon Kim, J. Yang, S.E. Yoo, and D. Kim, "Neighbor table based shortcut tree routing in ZigBee wireless networks", *IEEE Transactions* on *Parallel* and *Distributed Systems,* Vol. 25, No. 3, pp. 706–716, Mar. 2014.

[72]. T. Kim and D. Kim, "Opportunistic Shortcut Tree Routing in ZigBee Networks", *IEEE Sensors Journal*, Vol. 16, No. 12, pp.5107-5115, 2016.

[73]. Y. Li, W. Chen, and Z.L. Zhang, "Optimal forwarder list selection in opportunistic routing", *Proceedings of IEEE 6th International Conference on Mobile Adhoc Sensor System*, China, pp. 670–675, Oct. 2009.

[74]. E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks," *IEEE Transactions on Mobile Computing*, Vol. 8, No. 12, pp. 1622–1635, Dec. 2009.

[75]. N. Chakchouk, "A survey on opportunistic routing in wireless communication networks," *IEEE Communication Surveys Tutorials*, Vol. 17, No. 4, pp. 2214–2241, Nov. 2015

[76]. J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks" , *IEEE Transactions on Industrial Informatics*, Vol. 11, No. 1, pp. 112–121, Feb. 2015

LIST OF PUBLICATIONS

JOURNALS

1. Jegan. G and Samundiswary. P, "Energy Efficient Intrusion Detection System for ZigBee based Wireless Sensor Networks", *International Journal of Intelligent Engineering and Systems* (IJIES). Vol.10, No.3, pp. 155-165, 2017, ISSN: 2185-3118. (**Scopus Indexed**)

2. Jegan.G and Samundiswary. P, "Optimised watchdog system for detection of DDOS and wormhole attacks in IEEE802.15.4 based wireless sensor networks", *International Journal of. Mobile Network Design and Innovation,* Inderscience Publishers, Vol.7, No. 4, 2017, ISSN 1744-2850. (In press). (**Scopus Indexed**)

3. Jegan. G and Samundiswary. P, **"**Wormhole Attack Detection in Wireless Sensor Networks using Intrusion Detection System**",** *Indian Journal of Science and Technology*, Vol. 9, No.45, pp.1-10, December-2016, ISSN: 0974-684. (**Scopus Indexed)**

4. Jegan.G and Samundiswary. P, "Energy Efficient Intrusion Detection System based on Optimized Watchdog System and Hidden Markov Model for Wireless Sensor Networks", *International Journal of Control Theory and Applications*,Vol.8, No.5, pp. 1843-1852, 2015, ISSN : 0974-5572. (**Scopus Indexed**)

5. Jegan.G and Samundiswary. P, "Performance Evaluation of IEEE 802.15.4 based WSN using Routing Protocols under Wormhole Attacks", International *Journal of Applied Engineering Research*, Vol. 10 No. 20, pp. 19155-19159, 2015, ISSN 0973-4562. (**Scopus Indexed**)

CONFERENCES

1. Jegan. G and Samundiswary. P, "Optimized watchdog system for detection of wormhole attacks in IEEE802.15.4 based wireless sensor network" *in Proceedings of IEEE sponsored 3rd International Conference on Electronics and Communication Systems, Coimbatore*, Vol. 5, pp.2461-2466, Feb. 2016.

2. Jegan. G and Samundiswary. P, "A Comparative Study of Reactive, Proactive and Hybrid Routing Protocol in Wireless Sensor Network under Wormhole Attack", *in Proceedings of International Conference on Emerging Trends In Electrical and Communication Technologies*, Chennai, pp. 25, March 2017.

VITAE

G. Jegan was born on 27th September, 1984 in Karaikal district of Puducherry (U.T). He has received his B.Tech degree in Electronics and Communication Engineering (ECE) from Bharathiyar College of Engineering and Technology affiliated to Pondicherry University, in 2008. He has completed M.Tech. degree in ECE from Pondicherry Engineering College affiliated to Pondicherry University, puducherry, India in 2012. He has worked as Project Fellow under the UGC-India supported major research project for one year. Currently, he is pursuing Ph. D (full time) in the Department of Electronics Engineering of School of Engineering and Technology at Pondicherry University. His areas of interests include Wireless Sensor networks and wireless security.