Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/102866, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Wormhole Attack Detection in Zigbee Wireless Sensor Networks using Intrusion Detection System

G. Jegan and P. Samundiswary

Department of Electronics Engineering, Pondicherry University, Puducherry, India;
jeganece84@gmail.com, samundiswary_pdy@yahoo.com

Abstract

Objective: Wormhole attack is a serious threat to Wireless Sensor Networks (WSN) due to its wireless broadcast nature of communication, multi hop nature and resource constraints. Hence, to enhance the security and energy efficiency of a WSN, energy efficient Intrusion Detection System (IDS) is needed to detect and mitigate the attacks. In this paper, an Energy Efficient Intrusion Detection System (EE-IDS) has been proposed for IEEE 802.15.4 based WSN to detect and mitigate the effect of wormhole attacks. **Methods/Statistical Analysis:** The wormhole attack is detected by using the optimized watchdog system. The optimized watchdog mechanism is a trust based method which is used to evaluate the validity of all the nodes of the network. In proposed approach, the optimization has been done in the selection of watchdog nodes, in order to consume less energy compared to that of the existing approaches. The detection of wormhole attack is also completely relies on the three main factors like trustworthiness, packet delivery ratio and end-to-end delay. **Findings:** The proposed EE-IDS is examined through extensive simulations by considering static and mobility model, and then it is compared with the existing IDS for detecting wormhole attacks. The performance of zigbee WSN is analyzed in terms of metrics such as packet delivery ratio, average end-to-end delay and energy consumption for static model. In mobility model, the Proposed EE-IDS is evaluated in terms of detection rate, false positive rate and detection time. **Application/ Improvements:** The proposed EE-IDS is used to detect the wormhole attack and improve the energy efficiency in zigbee based wireless sensor networks, which can be used for military, environmental, health and commercial applications.

Keywords: IEEE802.15.4 based WSN, Intrusion Detection System, Optimized Watchdog, Wormhole Attack

1. Introduction

WSNs are emerging as a promising platform for variety of applications ranging from health care to tactical military applications. Although WSN's have many attractive features like low cost, less complexity and lower consumption of energy, WSN are exposed to a wide range of security attacks due to their open nature of the wireless communication channels and deployment of nodes in hostile environments. Among these attacks, wormhole attack is one of the devastating routing attacks that is hard to detect because they use a private out-of-band channel which is invisible to the WSN. Even though, security approaches such as authentication, cryptography or key management techniques build up the WSNs security, they are not preventing attacks[1-3] such as DoS (Denial of Service) and hole attacks effectively. One practical security defense scheme namely Intrusion Detection System[4-6] (IDS) is needed for the prevention of such types of attacks, because existing security mechanisms are not effective against such attacks and also not suitable for resource constraint network. A system which is capable of identifying the malicious nodes and then quickly reports the neighboring nodes to perform counter action is called as the Intrusion Detection System (IDS). In trust based IDS, watchdog[7-8] is a malicious node detection mechanism by observing the behavior of the node in the network. In WSN safety, watchdog is a basic part of the trust processes. However the energy consumed by the watchdog is very high and therefore reduces the lifetime of the

*Author for correspondence

network. Even though existing IDS are used for ad-hoc networks and wired, it is impracticable to apply directly in resource constrain network namely zigbee WSN, mainly because of the huge variation in their network characteristics such as, lifetime, autonomy, deployment location and self-configurability. It is also a fact that if the network size is bigger, the amount of data being generated is also huge, which makes real time prediction a difficult task. Thus, zigbee based WSNs require a novel and lightweight design of IDS. Many security mechanisms have developed to protect against wormhole attacks in wireless ad hoc and sensor networks.

In paper[10], authors have considered packet leashes – geographic and temporal information. This technique necessitates tight clock synchronizations, and thus it is difficult to achieve with resource constrained network such as zigbee WSN.

S. Capkun et al.[11] have proposed the SECure tracking Of node encounteRs (SECTOR) protocol to defend against wormhole attacks. Since it uses packet leashes, the energy consumption is more and not suitable for resource constrained network.

L.Hu and Evans D[12] have introduced a directional neighbor discovery protocol to defend against wormhole attacks by introducing directional antennas into a network. Although this method decreases the threat of wormhole attacks, use of directional antennas by all the nodes consume more energy.

There are few other techniques developed in the literature[13-14] to prevent wormhole attacks. However, these approach requires special hardware and tight clock synchronization among the sensor nodes to prevent the attack.

Among the existing works based on watchdog, the paper[7] discusses about insider threats against trust mechanism with watchdog and counter measures in wireless sensor networks.

The author's in paper[8] have presented an advanced watchdog mechanism for identifying the malicious nodes on the basis of a power aware hierarchical model. In this mechanism, the cluster head take up the role of the watchdog. This mechanism faces the issue of storage overhead and buffer overflow because every message has to be managed by the cluster head.

Peng Zhou et al.[9] have presented a collection of optimization techniques to reduce the energy consumption of watchdog utilization, when maintaining the security of the network at appropriate level. It includes the theoretical analyses along with the practical algorithms which are capable of scheduling the several tasks of the watchdog based on the position of the node and also the trustworthiness of the destination nodes.

Yanzhi Ren et al[15]. proposed a detection mechanism for wormhole attacks in Delay-Tolerant Networks (DTN). This approach exploits the existence of a forbidden topology in the network. Even though this approach detected wormhole attacks in effectively in DTNs for zebranet mobility models and random way point model, it has achieved only 92% of detection rate.

In this work, a novel approach called EE-IDS used to detect the wormhole attacks in IEEE802.15.4 based WSN is proposed. The core part of EE-IDS is the optimized watchdog system[9], which is a trust based intrusion detection technique that identifies the malicious nodes and its activities in the network to monitor the nodes within its communication range. The nodes selected as the watchdog node by the sink are the most trustworthy nodes due to its inherent features like highly stable. When any node transmits its data packet towards its destination node through the intermediate nodes, the watchdog present within the communication range of the transmitting node and intermediate node can determine the data packet that is being transmitted by the intermediate node or not, thus the watchdog node is checking the validity of the nodes involved in the transmission of the data packet. This is due to the fact that, when the source node forwards its packet to the desired intermediate node, along with this desired node, many other surrounding nodes within the communication range of the sending node receives this data packet. The nodes which are receiving the data packet will simply drop the data packet if they are not the desired intermediate node. But, when the watchdog node receives this data packet, it utilizes this packet for intrusion detection.

The approach described in this article is completely based on three factors such as trustworthiness, end-to-end delay and PDR for the detection of wormhole attacks. Since proposed approach relies on the watchdog technique, the certain nodes in the network will be selected as watchdog to monitors the behavior of the neighbor's node. The selection of watchdog nodes is based on some conditions which are given in detail in section-3. Finally the proposed method is validated by comparing the performance metrics such as detection rate, average

detection time, False Positive Rate (FPR), PDR, delay and energy consumption with the existing IDS[15,9] for mobility model and static model.

The rest of this paper is organized as follows. Section-2 illustrates the wormhole attack in WSN. In section-3 the proposed EE-IDS for detection of wormhole attacks using Optimized Watchdog System is given. Section-4 discusses about the simulation result and finally section-5 concludes the paper based on findings and analysis.

2. Wormhole Attack

Wormhole attack[16] is an attack on the routing protocols in WSN. In this attack, the attacking nodes develop an illusion that two nodes at different ends of the network are linked through few nodes which are neighbors. But in reality, the linking nodes which look like neighbors are actually not neighbors and are situated far away from each other. The virtual link is created by connecting the supposed neighbors by means of a concealed channel. As a result, in this attack, the malicious nodes can attack from two spots which lie at two different ends. Since, the distant nodes appear to be connected through few intermediate neighboring nodes, the traffic through this path increases at a higher rate. The attacker takes advantage of this situation and degrades the network performance drastically.

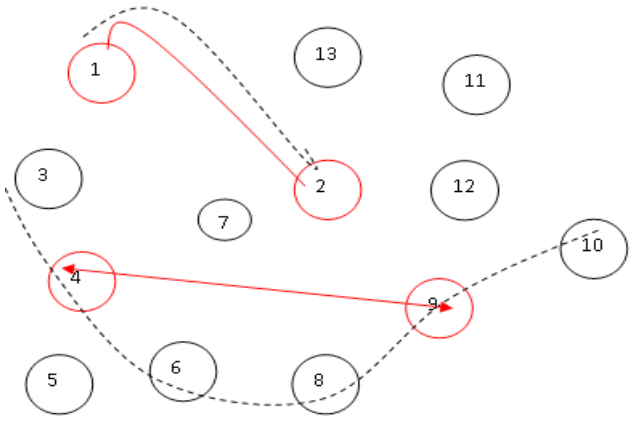

Figure 1. Wormhole attack.

Figure 1 describes the wormhole attack where node 1, 2, 4 and 9 are wormhole attacker nodes. Node 4 and 9 advertizes that they are neighbors, which makes the routing protocol to fail and establish routes when they are not actually neighbors, then start transmit the data through a short path but in reality the path followed is through node 3, 6, 8 and 10. Thus by making false routing, it perform man-in-the middle attack, maliciously dropping the packets, attract the network traffic towards it and eavesdrop on data traffic to degrade the network performance.

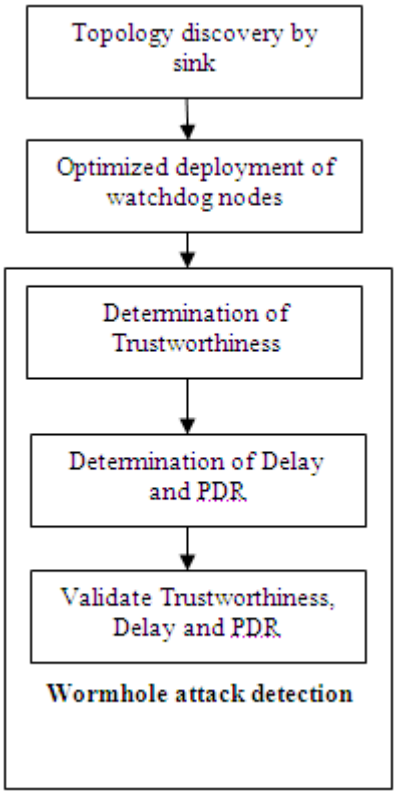

Figure 2. Functional flow diagram of proposed EE-IDS.

3. Proposed EE-IDS for Wormhole Detection

3.1 Overview

In this work, the optimized watchdog trust system[9] for detecting the wormhole attacks has been extended. The Figure-2 illustrates the functional block diagram of proposed EE-IDS for detection of wormhole attack. It consists of three main phases, they are topology discovery, optimized deployment of watchdog nodes and detection of wormhole attack. A topology discovery phase is conducted by the sink node 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 is discussed, which is clearly explained in the following section. Then the

wormhole attack detection is based on the three factors such as trustworthiness of the nodes, the abnormal variation in the end to end delay and Packet Delivery Ratio (PDR). Here each watchdog node estimates the trustworthiness of node by collecting the hop by hop queuing delay and received traffic. Figure 2 illustrates the functional flow diagram of the proposed EE-IDS.

3.2 Topology Discovery Mechanism

Step 1

The sink periodically broadcasts a topology message to all the sensor nodes in the network.

Step 2

By receiving the topology message, every node measures QoS metrics such as the Queue Delay (QD) and residual energy (E_R) of its neighbor nodes.

Step 3

After the measurement of quality of service metrics, each node gathers information about 1-hop and 2-hop neighbor nodes and stores in a Topology Information Table (TIT) as shown in Table 1.

Table 1. Topology Information Table (TIT)

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

Step 4

The TIT value is broadcasted again towards the sink by the nodes for updating their information to the sink.

3.3 Location Optimization of Watchdog Nodes

Consider a WSN with flat topology and its system model M= (N, E) as shown in figure 3, where $n_i \in N$ represents a sensor node in WSN and $e_{ij} \in E$ means that the nodes n_i and n_j are neighborhood (i.e., which are exist within each other's communication range). Let r_i be the communication range of n_i, and $e_{ij} \in E$ exists only if $d_{ij} \leq r_i$ and $d_{ij} \leq r_j$. Let $Bi=\{n_j \mid e_{ij} \in N\}= \{nj \mid dij \leq ri \ \& \ d_{ij} \leq r_j\}$, $Bi \in N$ is defined as the set of n_i's neighborhood nodes. Although n_3 and n_4 are exist within n_2's communication range (i.e., $d_{23} \leq r_2$ and $d_{24} \leq r_2$), e_{23} and e_{24} do not exist (i.e., $n_3, n_4 \in B_2$) because $d_{23} > r3$ and $d_{24} > r_4$.

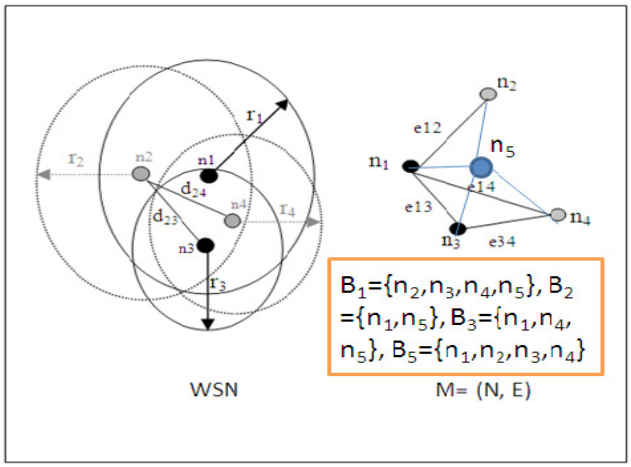

Figure 3. A WSN and the system model M.

Watchdog techniques are optimized to minimize the energy consumption of the entire WSN and to maximize security in terms of trustworthiness, detection rate, false positive rate and detection time. To achieve optimization, an appropriate set of cooperative watchdog nodes (W_j) must be found. This problem is to select the nodes from each target nodes neighbor to carry out watchdog task and to schedule watchdog tasks among the selected watchdog nodes. Let n_i and n_j be the nodes within the communication range and d_{ij} be the spatial distance between n_i and n_i. The node n_i can work as a watchdog to monitor only $\forall nj \in B_i$, and vice versa, only $\forall nj \in B_i$ can carry out watchdog tasks to monitor n_i. The nodes that are located close to the optimal d_{ij} and having highest residual energy with maximum number of neighbor nodes must be selected as watchdog nodes. From the system model M, the node n_5 is selected as the watchdog node (W_5) based on the above condition satisfied. Hence, the problem of finding optimal 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. When the attacker nodes are treated as watchdogs, then the security goal is not attained. Hence, the optimal watchdog location d_{ij} can be determined by considering the overall risk, which considers both security and energy consumption.

3.4 Wormhole Attack Detection

In the detection of the wormhole attack, a combination of the active and passive detection technique is applied. In the passive technique, additional data traffic is not added into the network and attack is detected on the basis

of the abnormalities detected by the passive monitors. In the active technique, regular probe traffic is transmitted into the network to gather the end to end statistics and deduce the network health and then the network validity is accordingly decided.

Three main factors are considered for the detection of wormhole attack. They are node trustworthiness, the abnormal variation in the packet delivery ratio (PDR) and average end-to- end delay. The most stable node in the network (a node which is having highest residual energy and more neighbor nodes) is selected as the watchdog. The hop by hop queuing delay is the delay experienced by a data packet at each node as it waits for its turn, to be transmitted to the next node along the path to its destination. The link which is experiencing abnormal variation in end-to-end delay is suspected as wormhole attack. Finally in the proposed approach, the wormhole verification is performed on such suspicious links by exchanging control packets[16] such as $HELLO_{req}$, $HELLO_{rep}$, probing packet and $ACK_{prob.}$

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

$$T_{ij} = \frac{\sum_{t \in N\, v\, w_{ij}^{t} \# \emptyset} K_{ij}^{t}}{\sum_{t \in N\, v\, w_{ij}^{t} \# \emptyset} 1} \quad (1)$$

Where,

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

K^{t}_{ij} : The event to represent nj's behavior is anticipated by ni at time slot t.

T : Time window.

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

The equation for end to end delay, D

$$D = N\,[D_{Tran} + D_{Prop} + D_{Proc}] \quad (2)$$

Where,

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

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

D_{Proc} : Time taken by the node to accept the packet, determine the next node along the transmission path and forward it to the determined node

D_{Tran} : Transmission Delay given by

$$D_{Tran} = N/R$$

Where, N is the number of bits in the data packet **R** is the rate of transmission

The equation for Packet Delivery Ratio (PDR) is

$$PDR = \frac{total\ packets\ received}{total\ packets\ sent\ \ by\ source} \quad (3)$$

The following algorithm and flowchart in Figure 4 describes the wormhole detection technique in WSN.

3.5 Algorithm

The proposed algorithm is described below and the notations used are:

- *D* : End- to- End Delay
- *PDR* : Packet Delivery Ratio
- *SD* : Standard Deviation
- *TD* : Topology Discovery
- *M* : Watchdog node
- $D_{Watchdog}$: End to end delay estimated by the watchdog
- $PDR_{Watchdog}$: PDR estimated by the watchdog
- D_{Sink} : End to end delay estimated by the sink
- PDR_{Sink} : PDR estimated by the sink

i. The *M* determines the trustworthiness of every node in the network based on the hop by hop queuing delay and received traffic.

ii. Each node transmits probes to its 3 hop neighbors and records the average *D*, also estimates the *PDR* along the path between the 3 hop nodes.

iii. The recorded values are collected by *M* at regular intervals of time.

iv. Based on the received values, M determines the trustworthiness of each node by correlating the values obtained from different nodes and also estimates a practical $D_{watchdog}$ and $PDR_{watchdog}$ value faced by the data packet.

v. On receiving the data packet, the destination node i.e., the sink performs *TD* using the *TD* agents and records the observed statistics with respect to *D* and *PDR*.

vi. Based on the observed statistics, the dependency between the nodes and end to end paths are determined and thus, the D_{sink} and PDR_{sink} value is also estimated.

vii. If $D_{watchdog} = D_{sink}$, and $PDR_{watchdog} = PDR_{sink}$, and trustworthiness =1, then no attack is detected. If $D_{watchdog} \neq D_{sink}$, or/and $PDR_{watchdog} \neq PDR_{sink}$, then wormhole attack is suspected. Finally, the suspicious link is verified by watchdog nodes using exchanging control packets between the suspicious node and M.

viii. Finally, after detecting the wormhole attacks, the communication link of wormhole nodes will be disconnected from the network to completely mitigate the affect of attacks.

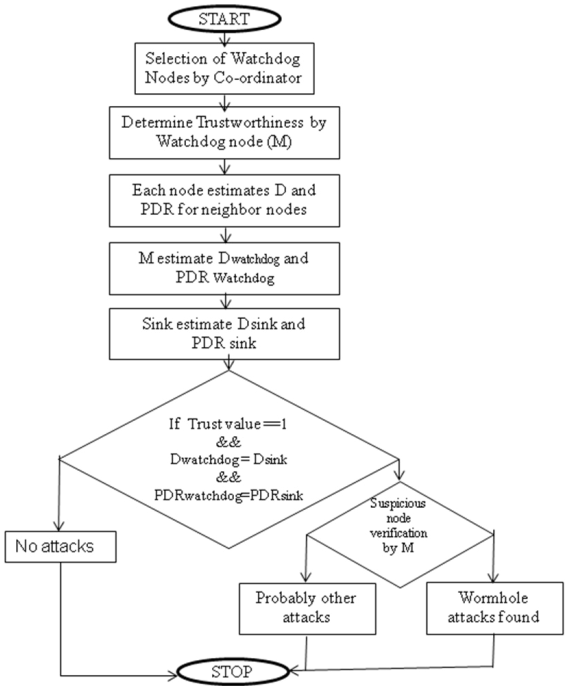

Figure 4. Flowchart for wormhole detection.

4. Simulation Results

4.1 Simulation Setup

The proposed and existing systems are evaluated by using NS2 simulations[17]. In this simulation, the performance of the network by considering two different scenarios is evaluated. In first scenario, the area of node deployment is 1500 x 1500 m^2 with 100 number of nodes deployed randomly, and second scenario consists of 100 number of static nodes deployed over the terrain area of size 100x100 m^2. The maximum transmission range of a node is set to 100 meter for the first scenario and 10 meter for second scenario. The wormhole attacker node is deployed randomly into the formed network in mobility model. The effectiveness of proposed approach has been evaluated in terms of detection rate, false positive rate as well as average detection time by varying node density and number of wormholes inside the network for mobility model in the first scenario. In second scenario, the performance of zigbee WSN is analyzed by using proposed EE-IDS with three different routing protocols such as AODV, Shortcut Tree Routing (STR) and Opportunistic Short cut Tree Routing (OSTR) in terms of packet delivery ratio, average end-to-end delay and energy consumption for the static model. In the second scenarios, the attacker launch is varied as 1, 2, 3, 4 and 5. Finally, the simulation results of the proposed system are compared with the existing approach[15] for mobility model and existing Energy Efficient Trust System[9] (EE-TS) for static model. The simulation parameters configuration details are given in Table 2.

Table 2. Simulation parameters

No. of Nodes	**20,40,60,80,100**
Area	100 X 100 m^2 , & 1500 X 1500 m^2
MAC	IEEE 802.15.4
Routing Protocol	AODV,STR,OSTR
Simulation Time	60 sec,180 sec
Mobility model	Random way point
Traffic Source	Poisson
Attackers	5 pair
Node energy	1Joule
Propagation	Two Ray Ground
Antenna	Omni directional Antenna

4.2 Performance Metrics of EE-IDS

The following performance metrics of the EE-IDS are evaluated and compared with the existing IDS.

- **Detection Rate (or) True Positive Rate:** It means the number of attacker node identified by the system divided by the total number of normal nodes present in the test set.

- **False Positive Rate:** It means normal node predicted as attacker node.
- **Average Detection Time:** Average time consumed by the IDS for detecting the attacker nodes

4.3 Results & Analysis

The descriptions of simulated results of proposed (EE-IDS) and existing IDS[15,9] method are presented in this section.

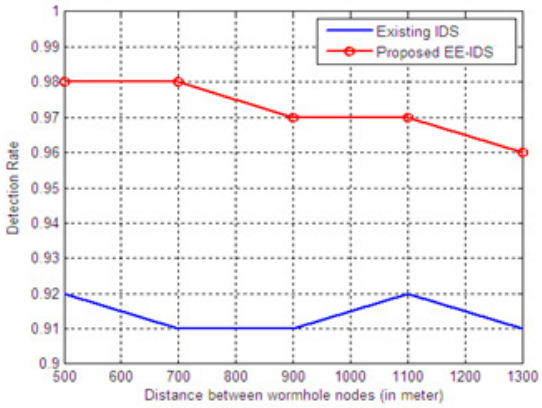

Figure 5. Detection rate when varying the distance wormhole nodes in mobility model.

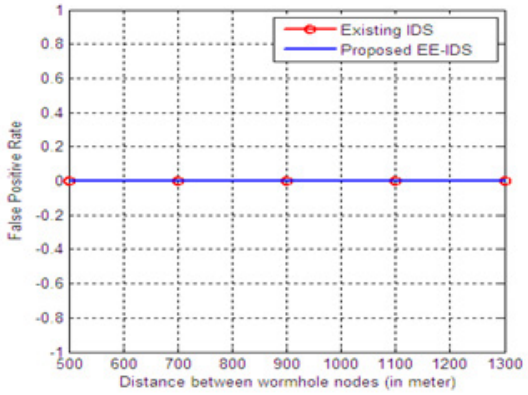

Figure 6. False positive rate when varying the distance between wormhole nodes in mobility model.

The simulation results shown from figures 5 to 7 illustrates the performance metrics such as detection time, false positive rate, average detection time with respect to distance between two wormhole nodes in mobility model of proposed EE-IDS and existing IDS. Figure 5 shows that detection rate of proposed method is better than that of the existing IDS. This is because of deployment of watchdog nodes in distributed manner which can be effectively monitors the behaviour of three hop neighbour nodes and also it updates the information about the neighbour's nodes to the sink node, so that wormhole attack can be detected efficiently with the help of information received by the watchdog nodes and sink nodes. Figure 6 depicts the False Positive Rate (FPR) as the function of distance between the two wormhole nodes in the mobility model of proposed and existing IDS. It is inferred from the simulation results that the FPR of both the system is zero, which means that both the systems are not detecting the normal nodes as attack nodes. From the Figure 7, it is clear that average detection time of proposed method is lesser than the existing IDS, but it is increasing with respect to distance between two wormhole nodes for both the system.

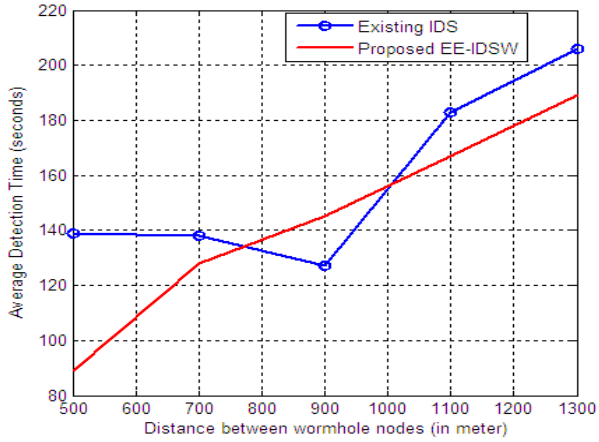

Figure 7. Average detection time when varying the distance between wormhole nodes in mobility model.

In proposed approach, detection time is increased w.r.t distance between the wormhole nodes. This is due to time taken by the distributed watchdog nodes for sending the processed data about the neighbour's node to the sink nodes for making the decision whether those nodes are normal nodes or attacker.

The simulation results of proposed method are shown from Figure 8 to 13. Figure 8 and 9 illustrates the packet delivery ratio of static WSN. The packet delivery ratio increases with respect to increased number of wormhole attacker and it is also clear that the proposed EE-IDS-AODV, EE-IDS-STR and EE-IDS-OSTR have better performance than that of the existing EE-TS by 19.4%, 34% and 46% respectively as shown in Figure 8.

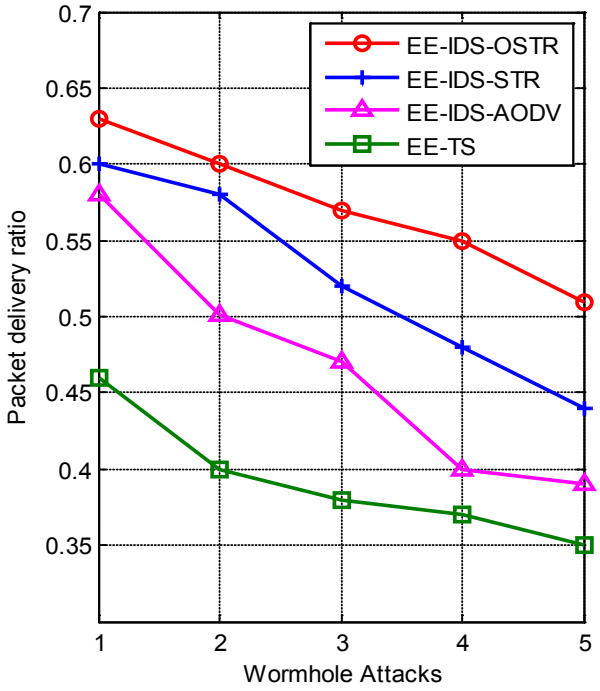

Figure 8. Packet delivery ratio when varying the number of wormhole attacks in static WSN.

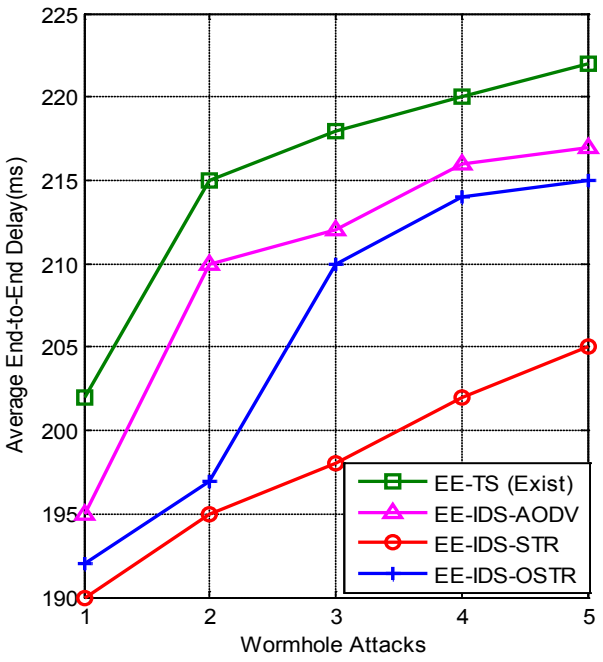

Figure 10. Average end-to-end delay when varying the number of wormhole attacks in static WSN.

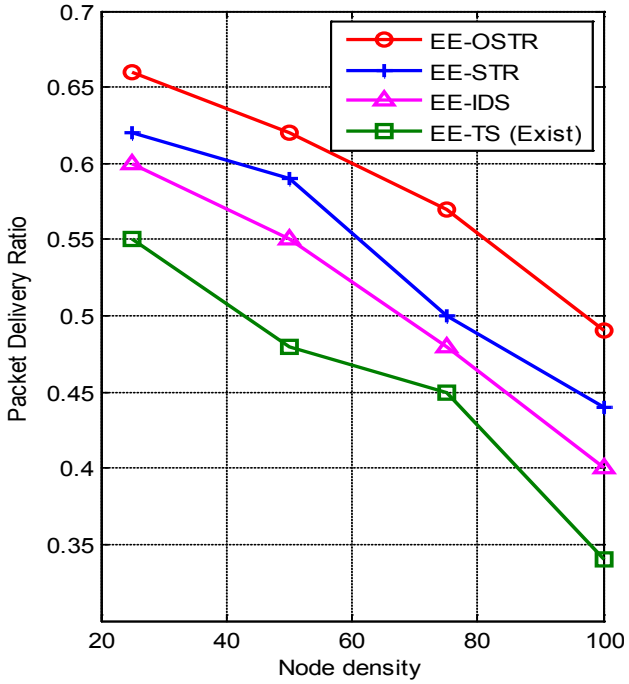

Figure 9. Packet delivery ratio when varying the number of nodes in static WSN in presence of 5 attacks.

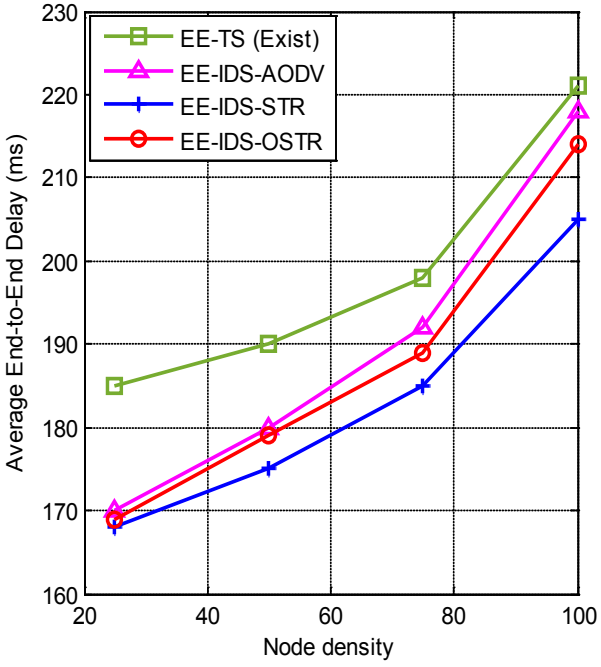

Figure 11. Average end-to-end delay when varying the number of nodes in static WSN in presence of 5 attacks.

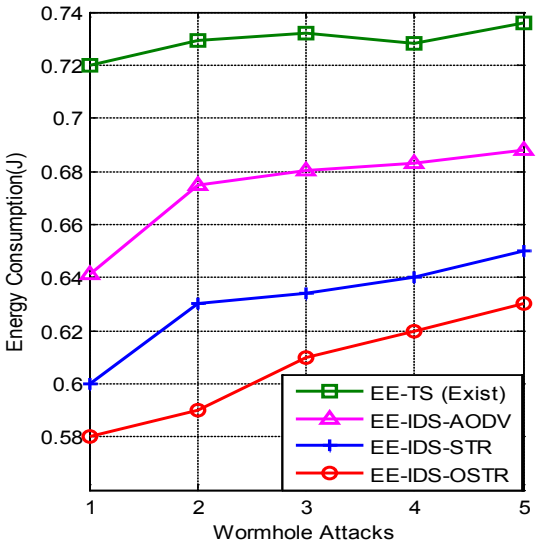

Figure 12. Energy consumption when varying the number of wormhole attacks in static WSN.

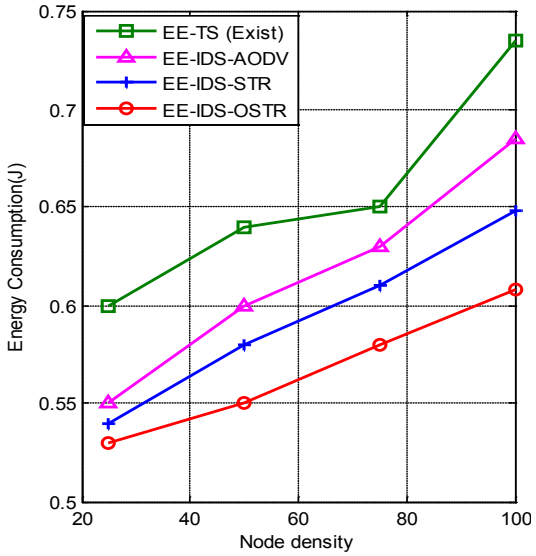

Figure 13. Energy consumption when varying the number of nodes in static WSN in presence of 5 attacks.

Similarly, the Figure 9 shows that PDR decreases w.r.t increased node density in presence of 5 attacks. It is inferred from the Figure 9 that, the proposed IDS namely EE-IDS-AODV EE-IDS-STR and EE-IDS-OSTR have shown improved performance by 9%, 14.36% and 24% respectively. Figure 10 and 11 shows the average end-to-end delay w.r.t wormhole attack and increased node density with presence of 5 attacks. It is observed from the Figure-10 that the proposed EE-IDS-AODV, EE-IDS-STR and EE-IDS-OSTR outperforms the existing IDS in terms of average end-to-end delay by reducing to 2.5 %, 8% and 4.5% respectively w.r.t increased wormhole attacks In Figure 11, the proposed EE-IDS-AODV and EE-IDS-STR have shown the improved performance in terms of average end-to-end delay by reducing to 4.2%, 7.6% and 5.4% respectively w.r.t node density. The energy consumption of proposed IDS has also shown improved performance than that of the existing IDS by reducing to 7.8 %, 13.47% and 16.8% respectively as shown in Figure-12. Similarly the improvement in average energy consumption has shown by reducing to 6%, 9.3% and 14% w.r.t nodes density in presence of 5 attacks as shown in Figure-13.

5. Conclusion

In this paper, the EE-IDS using optimized watchdog system has been proposed for detecting wormhole attacks in the IEEE 802.15.4 based WSN. Initially, the detection of the wormhole attack is done based on the determination of trustworthiness, end-to-end delay and PDR involved during the data transmission in the network. This attack is predicted by abnormal variation in the trustworthiness, delay and PDR, which is validated based on the watchdog mechanism. It is proved through the simulation results that EE-IDS has better performance than that of the existing IDS for mobility model in terms of detection rate, false positive rate and average detection time. The performance of zigbee based WSN has also analyzed by using proposed EE-IDS with three different routing protocols such as AODV, STR and OSTR in terms of metrics such as PDR, average end-to-end delay and energy consumption for static WSN. It is depicted through the simulation results that EE-IDS with OSTR routing protocol has shown overall better performance when compared to that of EE-IDS-AODV, EE-IDS-STR and existing EE-TS. Further this work will be extended for evaluating the proposed EE-IDS for various mobility models.

6. References

1. Colin P, Flynn O. Message Denial and Alteration on IEEE Low-Power Radio Networks. 4th IEEE International Conference on New Technologies, Mobility and Security (NTMS). 2011 January; p.1-5.
2. Radosveta Sokullu, Orhan Dagdeviren, Ilker Korkmaz. On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack. The Second International Conference on Sensor Technologies and Applications. 2008 August; p. 673-78.
3. X. Du and H.-H. Chen. Security in wireless sensor networks. IEEE Wireless Communications. 2008; 15(4):60–66.

4. Amudhavel J et al. A Survey on Intrusion Detection System: State of the Art Review. Indian Journal of Science and Technology. 2016 March; 9(11).
5. Sheela Evangelin Prasad SN, Srinath MV and Murtaza Saadique Basha. Intrusion Detection Systems, Tools and Techniques – An Overview. Indian Journal of Science and Technology. 2015 December; 8(35).
6. Uddin M, Alsaqour R, Abdelhaq R. Intrusion Detection System to Detect DDoS Attack in Gnutella hybrid P2P network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71-83.
7. 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. 2012; p.134-41.
8. Forootaninia1 A and Ghaznavi-Ghoushchi MB. An Improved Watchdog Technique Based on Power-Aware Hierarchical Design for Ids in Wireless Sensor Networks. International Journal of Network Security & Its Applications. 2012 July; 4(4):161-78.
9. Peng Zhou, Siwei Jiang, Athirai Irissappane, 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. 2015 March; 10(3):613-25.
10. Hu YC, Perrig A and Johnson B. Packet leashes: a defense against wormhole attacks in wireless networks. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. 2003 April; 3:1976-86.
11. Capkun S, Buttyn L and Hubaux JP. SECTOR: Secure tracking of node encounters in multi-hop wireless networks, 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN). 2003 October.
12. Hu L and Evans D. Using directional antennas to prevent wormhole attacks. Network and Distributed System Security Symposium (NDSS). 2004.
13. Lazos L et al. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. IEEE Wireless Communications and Networking Conference. 2005; 2:1193-99.
14. Khalil I, Bagchi S, and Shroff NB. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. International Conference on Dependable Systems and Networks (DSN'05). 2005 July; p. 612-21.
15. Yanzhi Ren et al. Detecting Wormhole Attacks in Delay-Tolerant Networks [Security and Privacy in Emerging Wireless Networks]. IEEE Wireless communications. 2010 October; 17(5):62-42.
16. Yih-Chun Hu, Adrian Perrig and David B Johnson. Wormhole Attacks in Wireless Networks. IEEE Journal on selected areas in communications. 2006 February; 24(2):370-80.
17. Network Simulator. Available from: http:///www.isi.edu/nsnam/ns.