Received: February 19, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Energy Efficient Intrusion Detection System for ZigBee based Wireless Sensor Networks

Jegan Govindasamy[1]* Samundiswary Punniakodi[1]

[1]*Department of Electronics Engineering*
Pondicherry University, India
* Corresponding author's Email: jeganece84@gmail.com

Abstract: Nowadays, ZigBee is one of the dominating standards for wireless sensor networks and Internet of Things (IoT) networks. Even though, the ZigBee standard is formed with low per-unit costs, security in mind and network resilience, existing security mechanisms are not effective to provide security and protection against wormhole attacks and Distributed Denial of Service (DDoS) attacks on networks such as WSN and IoT. They also introduce high consumption of energy, storage memory and processing. In this work, Energy Efficient Intrusion Detection System (EE-IDS) and Energy Efficient Intrusion Detection System with Energy Prediction (EE-IDSEP) are proposed for protection of ZigBee based wireless sensor networks in presence of wormhole attacks and (DDoS) attacks. The EE-IDS is developed and its performance is evaluated by considering three different routing protocols such as Ad hoc On-Demand Distance Vector (AODV), Shortcut Tree Routing (STR) and Opportunistic Shortcut Tree Routing (OSTR) to improve the security against wormhole attack and to mitigate the energy consumption of the sensor nodes in the ZigBee based wireless sensor networks. The proposed EE-IDS and EE-IDSEP are evaluated through extensive simulations by using NS2 and then compared with the existing Energy Efficient Trust System for Wormhole detection (EE-TSW) and Energy Efficient Trust System (EE-TS) for detection of DDoS attack. It is inferred from the simulation results that proposed IDS namely EE-IDS-AODV, EE-IDS-STR and EE-IDS-OSTR for detection of wormhole attack have better performance than that of existing EE-TSW and proposed system EE-IDSEP for detection of DDoS attack have also shown better performance than that of existing system EE-TS in terms of performance metrics such as Packet Delivery Ratio (PDR), Average End-to-End Delay, energy consumption, detection rate, average detection time and False Positive Rate (FPR).

Keywords: Energy efficient intrusion detection system, STR protocol, DDoS attacks, Wormhole attack.

1. Introduction

Nowadays, ZigBee based WSN's are increasingly used in several real world applications such as environmental control, military, health monitoring, habitat monitoring, home security networks and especially IOT networks. One of the major challenges of ZigBee based WSNs besides user and industry acceptance is security. Although ZigBee communication protocol provides many attractive features like low cost, low power consumption and low complexity, networks such as ZigBee based WSN and IOT networks are vulnerable to a wide range of security attacks due to their open nature of the wireless communication channels and deployment of nodes in hostile environments. So security is a fundamental requirement for these networks. Even though, security solutions like authentication, cryptography or key management techniques enhance the ZigBee based WSNs security, they are not suitable for resource constrained networks and also it consumes more energy for detection of attacks [1] such as DoS (Denial of Service) and hole attacks. If a network consists of multiple DOS attacks at a time, then it may leads to DDOS attacks. In context of WSN, the DDoS attacks such as resource depletion, energy exhaustion and flooding attacks are destructive to networks. In case of hole attacks, wormhole attack is one of the devastating routing attacks that are difficult to detect because they use a private out-of-band channel which is invisible to the WSN. In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network and then replays them into the network from that point.

In order to improve the security of ZigBee based WSN, the practical security defence scheme namely Intrusion Detection System [2-3] (IDS) is needed for the prevention of hole attacks and DDoS attacks, because traditional cryptography-based security mechanisms are not effective against such attacks. A system that is capable of identifying the malicious nodes and then quickly reports the neighbouring nodes to perform counter action is called as the Intrusion Detection System (IDS). The commonly used IDS is trust based IDS, in which watchdog [4-5] is used for malicious node detection for observing the behaviour of the node in the network. In WSN safety, watchdog is a basic part of the trust process. However the energy consumed by the watchdog is very high and therefore reduces the lifetime of the network. Existing security mechanisms require higher energy consumption and large memory to detect the attackers. So, they are not suitable for resource constrained networks. Hence it is needed to design a novel and lightweight energy efficient IDS for resource constrained ZigBee based WSN.

In this paper, an attempt has been made to develop a novel approach namely EE-IDS and EE-IDSEP in order to detect the wormhole attacks and DDoS (Energy Exhaustion) attacks in IEEE 802.15.4 based WSN. The performance of EE-IDS is evaluated with the three different routing protocols such as AODV, STR and OSTR. In addition, EE-IDSEP is also developed to detect DDoS attacks and various performance metrics of IDSEP are examined. The core part of EE-IDS and EE-IDSEP is the optimized watchdog system, which is a trust based intrusion detection technique that identifies the malicious nodes to monitor the activity of the nodes within its communication range. The nodes selected as the watchdog node are the most trustworthy nodes due to its inherent features like highly stable. These watchdog nodes are deployed in the network randomly just as any other node. Since this approach is based on the watchdog mechanism, the certain nodes in the network will be selected as watchdog to monitor the behaviour of the neighbour nodes. The selection of watchdog nodes is based on some conditions which are given in detail in section 3. Finally, the performance of proposed systems are compared with the existing IDS [12] in terms of performance metrics such as detection rate, average detection time, False Positive Rate (FPR), average end-to-end delay, Packet Delivery Ratio (PDR) and energy consumption.

The rest of this paper is organized as follows. In section 2, related works are given in detail. Section 3 discusses about the existing routing protocols such as AODV, STR and OSTR. In section 4, the proposed EE-IDS for detection of wormhole attacks using Optimized Watchdog System is described. Section 5 deals with the EE-IDSEP for detection of DDoS attacks. Simulation result and discussions are given in section 6 and finally section 7 concludes the paper based on findings and analysis.

2. Related works

In this section, the articles related to security mechanisms for detecting the wormhole attacks and DDoS attacks in the wireless sensor network has been given in detail. Y.C.Hu et al. [6] have considered packet leashes – geographic and temporal. This solution requires tight clock synchronizations and thus it is hard to achieve with the resource constrained nodes.

S. Capkun et al. [7] have proposed the SECure tracking Of node encounteRs (SECTOR) protocol to defend against wormhole attacks. In SECTOR, the Mutual Authentication with Distance Bounding (MAD) protocol is used. This approach is similar to packet leashes at high level, but it does not require location information or clock synchronization. But it still suffers from other limitations of the packet leashes technique.

L.Hu and Evans D. [8], have proposed a directional neighbour discovery protocol to prevent wormhole attacks by introducing directional antennas into a network. Although this method diminishes the threats of wormhole attacks, it requires all nodes to use directional antennas. There are some other techniques proposed in the literature [9]-[10] to prevent wormhole attacks. However, these methods requires special hardware and tight clock synchronization between nodes in the network to defend against the attack. Among the existing works based on watchdog, the author’s in paper [4] discusses about insider threats and counter measures in wireless sensor networks.

The authors of paper [5] have presented an advanced watchdog mechanism for identifying the malicious nodes based on a power aware hierarchical model. In this mechanism, the cluster head takes 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.

Yanzhi Ren et al. [11], have 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 has detected wormhole attacks effectively in DTNs, it has achieved only 92% of detection rate.

Peng Zhou et al. [12] have presented a collection of optimization techniques to reduce the energy cost due to watchdog utilization by maintaining the security of the network at appropriate level.

C. Balarengadurai et al [13] have proposed a detection and prediction technique against DDoS attacks in IEEE 802.15.4 based on the Fuzzy logic system. DDoS attack is detected by using fuzzy logic based on the energy consumed by the node, which is estimated by using the Fuzzy Based Detection and Prediction System (FBDPS).

Bernardo M. David et al [14] have presented a bayesian trust model developed to identify MAC layer attacks by introducing some parameters which are context-dependent along with a flexible ageing factor which enable the adaptive handling of this trust model by varying particular network conditions on the basis of some context parameters.

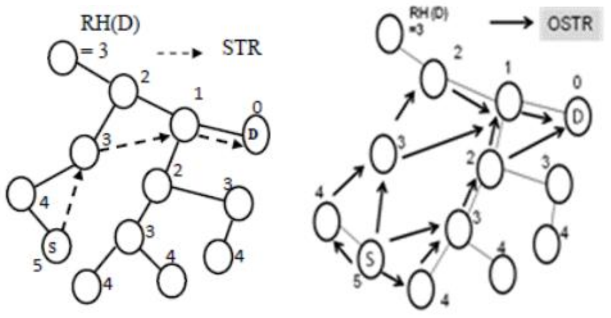
In paper [15-16], Jegan et al have developed EE-IDS and EE-IDSEP for detection of wormhole and DDoS attacks by using Ns2 simulator, and the performance of WSN is evaluated by considering the metrics such as PDR, average end-to-end delay and energy consumption. The simulation result shows that proposed IDS has better performance than the existing system for simulation time of 60s However, in that paper, the significant metrics such as detection rate, False Positive Rate (FPR) and detection time are not considered to evaluate the IDS.

In this paper, we have enhanced the previous work [15, 16] by considering the performance metrics of IDS such as detection rate, False Positive Rate (FPR) and detection time to evaluate the proposed and existing IDS by assuming simulation time of 100s.

3. Routing protocols

3.1 Ad hoc on-demand distance vector (AODV) routing

The AODV routing protocol [16] is intended for Mobile Ad hoc NETwork (MANET) and sensor networks. AODV is a reactive routing protocol. It uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. AODV has two basic operations: route discovery and route maintenance. AODV uses Route REQuest (RREQ), Route REPly (RREP) and Route ERRor (RERR) messages to find and maintain the routes.



(a) (b)

Figure.1 Routing: (a) STR Routing and (b) OSTR Routing.

3.2 STR and OSTR

The STR algorithm [17] is developed to solve the two problems of the Zigbee Tree Routing (ZTR) by using 1-hop neighbour information. The STR algorithm basically follows ZTR, but chooses one of neighbour nodes as the next hop node when the remaining tree hops to the destination can be reduced. In Fig. 1(a), the next hop node in STR is decided by a sender node (S); thus, a routing path cannot be changed even link failure or traffic congestion is occurred. On the contrary, the routing path of OSTR [17] in Fig. 1(b) can be adjustable according to traffic and link condition. OSTR can improve the reliability of PDR as well as efficiency of channel utilization due to dynamic participation of neighbour nodes.

4. Proposed EE-IDS with AODV, STR and OSTR routing protocol for wormhole attack detection

4.1 Overview

In this work, the optimized watchdog trust system [12] for detecting the wormhole attacks is extended. 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. In this phase, the routing protocols AODV, STR and OSTR

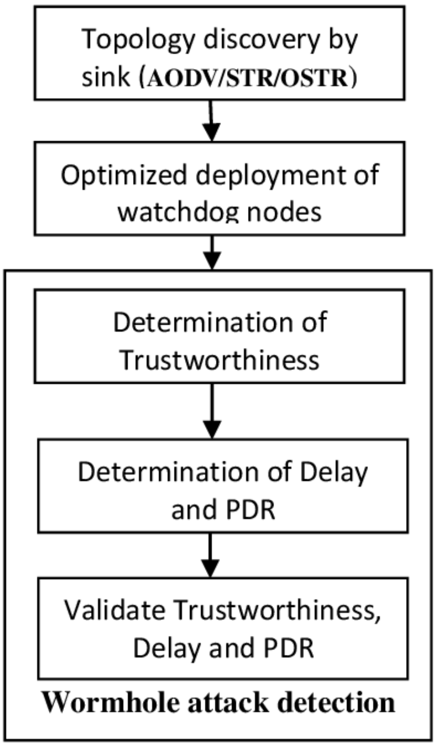

Topology discovery by sink (AODV/STR/OSTR)
Optimized deployment of watchdog nodes
Determination of Trustworthiness
Determination of Delay and PDR
Validate Trustworthiness, Delay and PDR
Wormhole attack detection

Figure.2 Functional flow diagram of proposed EE-IDS

have been used for routing. Following the topology discovery phase, optimized deployment of watchdog nodes is discussed, which is clearly explained in the following section. The wormhole attack detection is based on finding of 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.

4.2 Topology discovery mechanism

Step 1
The sink periodically broadcasts a topology message to all the 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 neighbour nodes.

Step 3
After the measurement of QoS metrics, each node gathers information about other nodes and stores in a Topology Information Table (TIT) as shown in table-1. Thus TIT holds the source node ID, 1-hop and 2-hop neighbour node ID, residual energy (E_R), and queue delay (QD) of each node along with the 2-hop neighbourhood information.

Table 1. Topology Information Table (TIT)

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

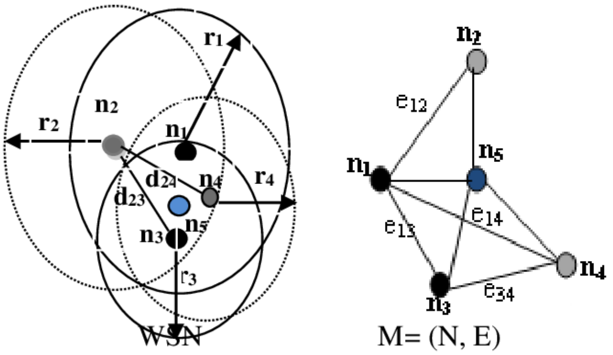


Figure.3 A WSN with the system model M

Step 4
The TIT value is broadcasted again towards the sink by the nodes and utilizing the updated node information; the topology is discovered by the sink.

4.3 Location optimization of watchdog nodes

Consider a WSN with flat topology and its system model M= (N, E) as shown in Fig. 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 neighbourhood (i.e., the nodes which are existing within each other's communication range). Let r_i 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 $B_i=\{n_j \mid e_{ij} \in N\}= \{n_j \mid d_{ij} \leq r_i \ \& \ d_{ij} \leq r_j\}$, $B_i \in$ N is defined as the set of n_i's neighbourhood 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 $\notin$ B_2) because $d_{23} > r_3$ and $d_{24} > r_4$.

Watchdog techniques are optimized to minimize the energy cost of the entire WSN and to maximize security in terms of trust worthiness. 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 neighbour to perform watchdog task and to schedule watchdog tasks among those selected watchdog nodes.

Let B_1= $\{n_2,n_3,n_4,n_5\}$, B2= $\{n_1,n_5\}$, $B_3=\{n_1,n_4,n_5\}$ $B_5=\{n_1,n_2,n_3,n_4\}$, n_i & n_j be the nodes within the communication range and d_{ij} be the spatial distance between n_i and n_j. The node n_i can work as a watchdog to monitor only $^{\forall}nj \in Bi$, and vice versa, only $^{\forall}$ nj $\in$ Bi can perform 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 that of 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.

4.4 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.

The main factors considered for the detection of wormhole attack are node trustworthiness, the abnormal variation in the end to end delay and Packet Delivery Ratio (PDR). The most stable node in the network (a node which is having highest residual energy and more neighbour 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 node experiencing end-to-end delay lesser than minimum threshold value is suspected as wormhole. Finally in proposed approach, the wormhole verification is performed on such suspicious links by exchanging control packets [18] such as HELLO*req*, HELLO*rep*, probing packet and ACK *prob.*

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

$$\mathrm{T_{ij}} = \frac{\Sigma_t \in \mathrm{Tv} W^t_{ij\neq 0} K^t_{ij}}{\Sigma_t \in \mathrm{Tv} W^t_{ij\neq 0} 1} \tag{1}$$

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 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 v_i expectation is satisfied by v_j's behavior, otherwise it will return 0.

The equation for end to end delay is given below.

$$\mathrm{D} = \mathrm{N}\left[\mathrm{D_{Tran}} + \mathrm{D_{prop}} + \mathrm{D_{Proc}}\right] \tag{2}$$

Where,

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

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

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

$$\mathrm{D_{Tran}} = \frac{\mathrm{L}}{\mathrm{R}} \tag{3}$$

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

The equation for Packet Delivery Ratio (PDR) is given by

$$\mathrm{PDR} = \frac{\text{Total Packets Received}}{\text{Total Packets Sent by Source}} \tag{4}$$

The following algorithm describes the wormhole detection technique in WSN.

Notations used:

❖ *D*	: End To End Delay
❖ *SD*	: Standard Deviation
❖ *TD*	: Topology Discovery
❖ W_N	: 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

Algorithm for Wormhole Detection

i. The W_N 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 2 hop neighbours and records the average *D*, also estimates the *PDR* along the path between the 2 hop nodes.

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

iv. Based on the received values, W_N 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. Then the sink compares the values estimated by it, with the values estimated by W_N.

viii. If $D_{Watchdog} = D_{Sink}$ && $PDR_{Watchdog} = PDR_{Sink}$ && trustworthiness = 1, then no attack is detected.

ix. 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 using exchanging control packets between the suspicious node and W_N.

x. 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 detected.

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.

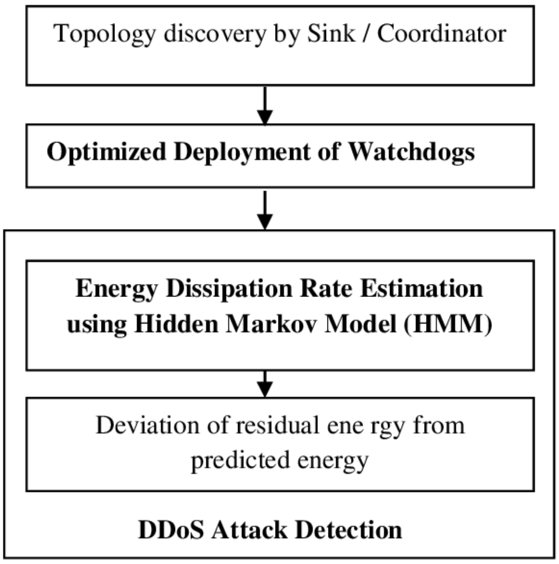

Topology discovery by Sink / Coordinator
Optimized Deployment of Watchdogs
Energy Dissipation Rate Estimation using Hidden Markov Model (HMM)
Deviation of residual ene rgy from predicted energy
DDoS Attack Detection

Figure.4 Functional flow diagram of proposed system EE-IDSEP

5. Proposed EE-IDSEP for detection of DDos attack

The DDoS attack includes resource depletion attack, energy exhaustion attack and flooding attack. In this paper, the energy exhaustion attack is considered as a DDoS attack. To identify this attack in the ZigBee WSN, the EE-IDSEP is developed, which consists of optimized watchdog system and Hidden Markov Model (HMM). The optimized watchdog system is used to monitor the activities of node. The energy dissipation rate of sensor nodes is predicted by applying the Hidden Markov Model [19] (HMM). The watchdog nodes collect the residual energies from the monitored nodes. It also estimates the actual energy consumed from the reported residual energies and compares them with predicted energy consumed values estimated by the HMM. The nodes with abnormal energy consumption are considered to be DDoS attacks with the aid of EE-IDSEP method. Figure 4 illustrates the functional flow diagram of the proposed system, which includes topology discovery by sink, optimized deployment of watchdogs and detection of DDoS attacks. The description of topology discovery by sink and optimized deployment of watchdogs are given in the previous section.

Notations:

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

Algorithm:

Step 1: Watchdog node estimates E_{consumed} using HMM filter
Step2: The watchdog collects the residual energy ($\mathbf{E}_{\text{Collected residual}}$) from all the monitored nodes.
Step-3: Watchdog estimates the $\mathbf{E}_{\text{Calculated residual}}$ (difference between the **initial energy** and E_{consumed} **)**
Step 4: If $\mathbf{E}_{\text{Collected residual}} \approx \mathbf{E}_{\text{Calculated residual}}$, then energy consumed is normal
Step 5: If $\mathbf{E}_{\text{Collected residual}} \neq \mathbf{E}_{\text{Calculated residual}}$, 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

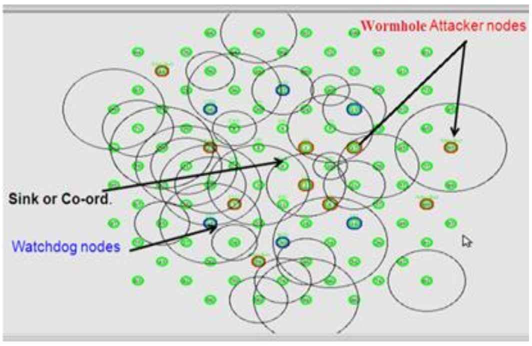


Figure.5 WSN scenario with wormholes attacks

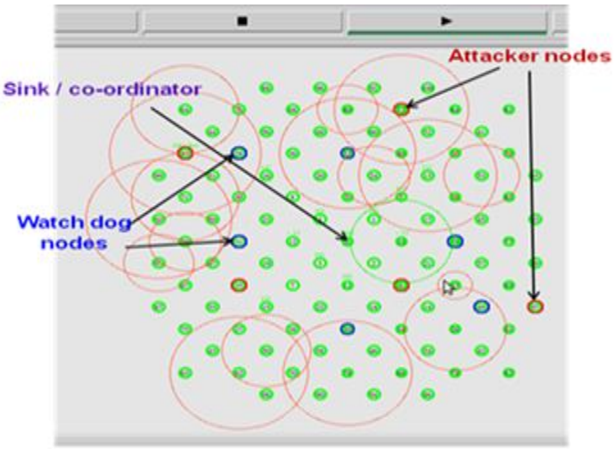


Figure.6 WSN scenario with DDoS attacks

Table 2. Simulation parameters

No. of Nodes	25, 50, 75, 100
Area	100 X 100 m^2,
MAC	IEEE 802.15.4
Routing Protocol	AODV, STR, OSTR
Simulation Time	100 sec
Traffic Source	Poisson
Attackers (DDoS & Wormhole attack)	5 &10 no’s
Node Energy	1 Joule
Propagation	Two Ray Ground
Antenna	Omni directional antenna

6. Simulation results

6.1 Performance evaluations

The proposed and existing IDS [12] are simulated by NS2 simulator. The parameters used for this simulation are shown in the table-2. The network consists of 100 number of nodes deployed randomly over the terrain area of size 100 x 100 m2. The wormhole attacker node pair and DDoS attacker nodes are deployed randomly into the formed network as shown in Figs. 5 and 6.

The effectiveness of proposed approach is evaluated 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 wormholes, DDoS attacks and node density. Finally, the simulation results of the proposed system namely EE-IDS and EE-IDSEP are compared with the existing EE-TSW and EE-TS.

6.2 Results and analysis

6.2.1. Proposed EE-IDS for wormhole detection

This section illustrates the simulation results of proposed EE-IDS and existing EE-TSW [12]. The simulation results shown from Figs. 7 to 9 depicts the packet delivery ratio, average end-to-end delay and energy consumption w.r.t number of wormhole attacks. Figures 10 to 12 illustrate the detection rate, false positive rate and average detection time of proposed and existing system.

It is clear from Fig. 7 that PDR decreases w.r.t increased wormhole attacks, also it is inferred from the result that proposed IDS namely EE-IDS-AODV, EE-IDS-STR and EE-IDS-OSTR have better performance than the existing EE-TSW by approximately 23%, 28% and 33% respectively. In Fig.8, proposed EE-IDS-AODV EE-IDS-STR and EE-IDS-OSTR have shown the improved performance in terms of reduced average end-to-end delay by approximately 5.4%, 8.8% and 6.6% respectively. Further, the proposed EE-IDS with AODV, STR and OSTR has also shown improved reduction in energy consumption than that of the existing EE-TSW by 0.3%, 10.3% and 12.3% respectively as depicted in Fig. 9.

The proposed IDS has better performance than that of existing system which is due to the optimized selection of distributed watchdog nodes, security mechanisms which includes combination of active and passive monitoring techniques and the influence of routing protocols. These makes the proposed system to detect the wormhole attacker nodes very earlier than existing system (i.e.,) 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 affect of attacker nodes in the network with respect to time. Thus the proposed system reduces the influence of attacker nodes in the network to improve the performance metrics such as PDR, energy consumption and average end-to-end

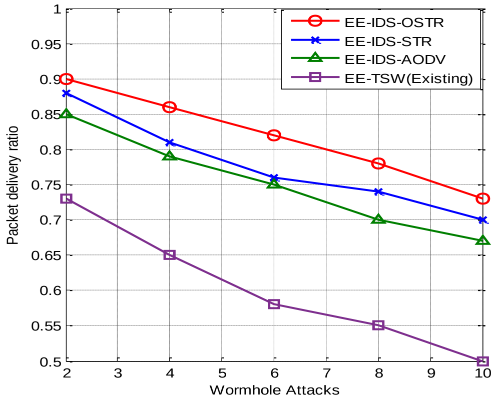


Figure.7 Packet delivery ratio Versus Attacks

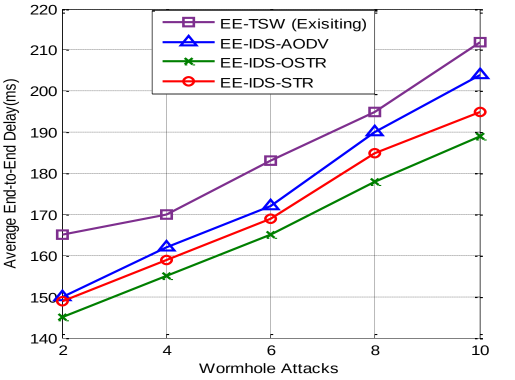


Figure.8 Avg. End-to-End Delay Versus Attacks.

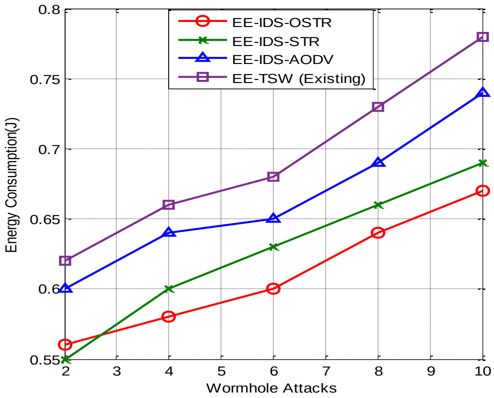


Figure.9 Energy consumption Versus Attacks

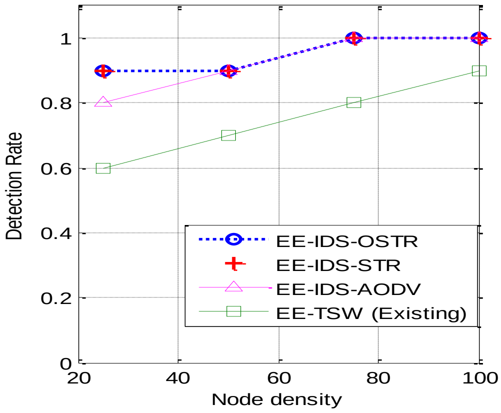


Figure.10 Detection rate Versus Node density

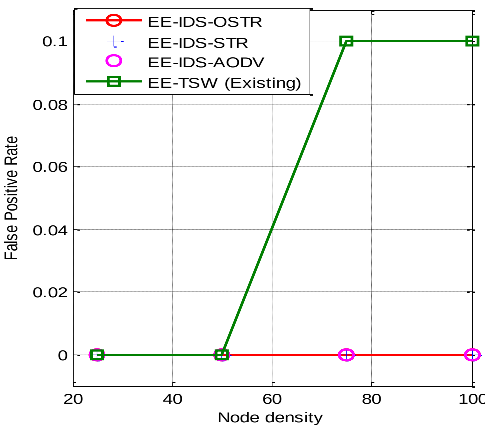


Figure.11 False Positive Rate Versus Node density

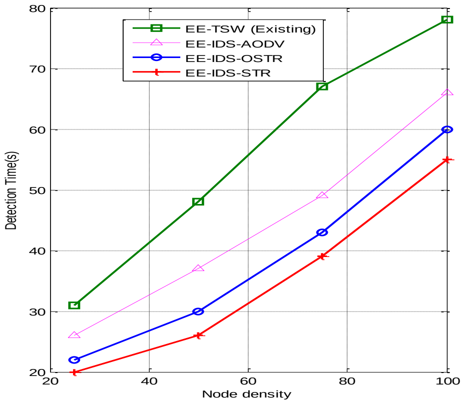


Figure.12 Detection time Versus Node density

delay. Even though the EE-IDS-AODV, EE-IDS-STR and EE-IDS-OSTR have same security mechanism, the EE-IDS with STR and OSTR protocol has shown better performance in terms of packet delivery ratio, average end-to-end delay and energy consumption compared to that of EE-IDS-AODV. This is due to the better routing performance of STR and OSTR, which includes less routing overhead, low memory consumption and lesser latency when compared to that of AODV. AODV is the reactive routing protocol which discovers the routing path only when there is request on packet delivery; thus, routing overhead of AODV and memory consumption is more when compared to that of STR and OSTR. The significant performance metrics of IDS such as detection rate, false positive rate and average detection time are illustrated from Figs. 10 to 12 respectively. The detection rate or true positive rate is shown in Fig. 10, 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 inferred from Fig.10 that the detection rate decreases w.r.t increased node density for existing and proposed IDS. The FPR of proposed IDS shown in Fig.11 refers to normal events predicted as attackers. It is observed that proposed system has 0% FPR when compared to that of existing system. Similarly the detection time of proposed system consume less time for detection of wormhole attack as shown in Fig. 12.

From the simulation results, it is inferred that, the proposed IDS with STR and OSTR protocol have shown better overall performance than that of the proposed EE-IDS with AODV and existing EE-TSW comparatively.

6.2.2. Proposed EE-IDSEP for DDoS attack

This section illustrates the simulation results of proposed EE-IDSEP and existing system EE-TS [12]. The simulation results shown from Figs. 13 to 15 depict the packet delivery ratio, average end-to-end delay and energy consumption w.r.t number of DDoS attacks. Figures 16 to 18 illustrate the detection rate, false positive rate and average detection time of proposed and existing system.

It is observed through the simulation results that proposed EE-IDSEP outperforms the EE-TS by approximately 10% improvement in terms of packet delivery ratio, 10% reduction in terms of end-to-end delay and 15% reduction in terms of energy consumption with respect to DDoS attacks. The performance metrics to evaluate the EE-IDSEP such as detection rate, False Positive Rate (FPR) and detection time have also shown better performance than that of existing system EE-TS.

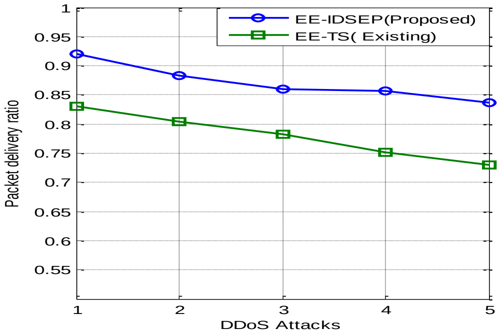


Figure.13 Packet delivery ratio Versus Attacks

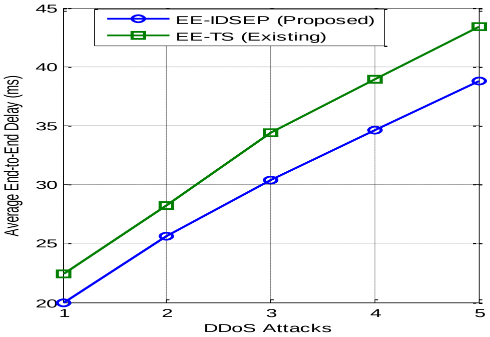


Figure.14 Avg. End-to-End Delay versus Attacks.

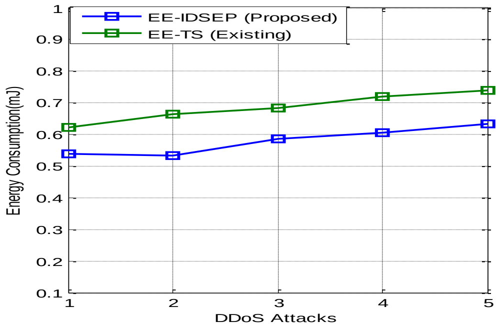


Figure.15 Energy consumption Versus Attacks

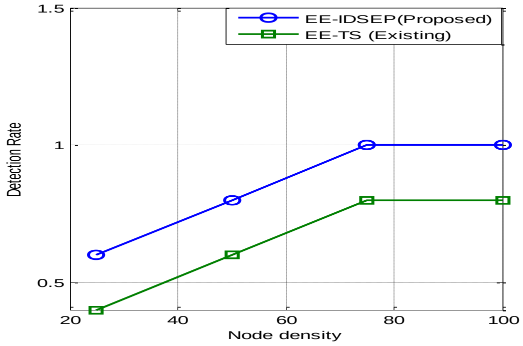


Figure.16 Detection rate Versus Node density

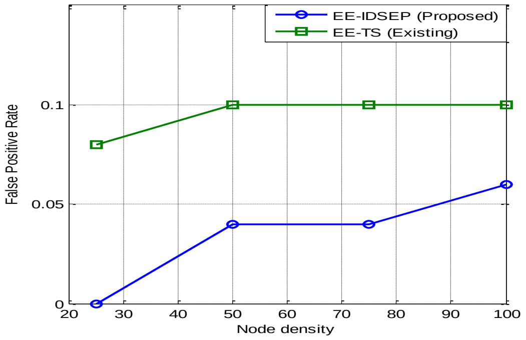


Figure.17 False Positive Rate Versus Node density

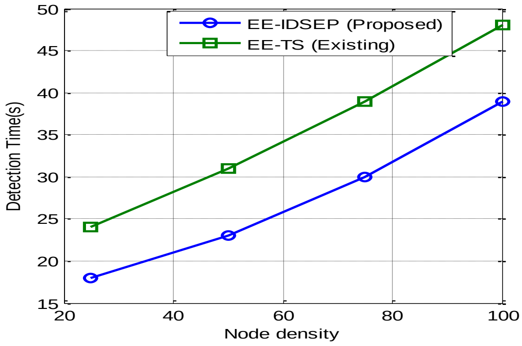


Figure.18 Detection time Versus Node density

7. Conclusion

In this paper, the EE-IDS and EE-IDSEP are proposed for detecting the wormhole attack and DDoS attack in ZigBee based wireless sensor network. It is proved through the simulation results that EE-IDS with STR and OSTR protocol have better overall performance than the existing EE-TSW by approximately 28% and 33% improvement in terms of packet delivery ratio, 8.8% & 6.6% reduction in terms of end-to-end delay and 10.5% & 12.3% reduction in terms of energy consumption w.r.t wormhole attacks. Similarly, proposed EE-IDSEP outperforms the EE-TS by approximately 10% improvement in packet delivery ratio, 10% reduction in end-to-end delay and 15% reduction in terms of energy consumption w.r.t DDoS attacks. The significant performance metrics of IDS such as detection rate, false positive rate and average detection time of proposed IDS have also shown better performance than the existing IDS. Hence it is concluded that the EE-IDS and EE-IDSEP can be utilized in many ZigBee applications requiring high security and less energy consumption. Further this work can be extended for mobility model of ZigBee WSN to detect the wormhole and DDoS attacks.

References

[1] X. Du and H.-H. Chen. “Security in wireless sensor networks”, *IEEE Wireless Communications*, Vol.15, No. 4, pp. 60-66, 2008.

[2] I. Butun, S. D. Morgera, and R. 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.

[3] J. Amudhavel et al, “A Survey on Intrusion Detection System: State of the Art Review”, *Indian Journal of Science and Technology*, Vol 9, issue 11, 2016.

[4] Y. Cho, G. Qu, Y. 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.

[5] A. Forootaninial 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, 2012.

[6] Y. C. Hu, Perrig A, and Johnson B. “Packet leashes: a defense against wormhole attacks in wireless networks”, In: *Proc. of INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, Vol.3, pp.1976 – 1986, 2003.

[7] S. Capkun, L. Buttyn and J.P. Hubaux, “SECTOR: Secure tracking of node encounters in multi-hop wireless networks”, In *Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2003.

[8] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks”, In: *Proc. of Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, 2004.

[9] L. Lazos *et al.*, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach”, In: *Proc. of IEEE Wireless Communications and Networking Conference*, Vol. 2, pp.1193 – 1199, 2005.

[10] I. Khalil, S. Bagchi, and N.B. Shroff, “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, In: *Proc. of the International Conference on Dependable Systems and Networks (DSN'05)*, pp. 612 – 621, 2005.

[11] R. Yanzhi et al, “Detecting Wormhole Attacks in Delay-Tolerant Networks (Security and Privacy in Emerging Wireless Networks)”, *IEEE Wireless communications*, Vol.17, No.5, pp 62-42, 2010.

[12] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. 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, 2015.

[13] C. Balarengadurai and 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, 2013.

[14] B. M. David, B. Santana, L. Peotta, M. D. Holtz, and R. T. Sousa Jr, “A Context-Dependent Trust Model for the MAC Layer in LR-WPANs”, *International Journal on Computer Science and Engineering*, Vol.2, No.9, pp. 3007-3016, 2010.

[15] G. Jegan and P. Samundiswary “Wormhole Attack Detection in Zigbee Wireless Sensor Networks using Intrusion Detection System” *Indian Journal of Science and Technology*, Vol.9, No. 45, pp. 1-10, 2016.

[16] G. Jegan and P. Samundiswary “Energy Efficient Intrusion Detection System based on Optimized Watchdog System and Hidden Markov Model for Wireless Sensor Networks”, *International Journal of Control Theory and*

Application (IJCTA) , Vol.8, No.5, pp. 1843-1852, 2015.

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

[18] 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.