I J C T A, 8(5), 2015, pp. 1843-1852

Energy Efficient Intrusion Detection System based on Optimized Watchdog System and Hidden Markov Model for Wireless Sensor Networks

G. Jegan* and P. Samundiswary**

Abstract: Wireless Sensor Network (WSN) is one of the most propitious technologies with many applications ranging from health care to tactical military applications. Although Wireless Sensor Networks have many attractive features like low cost, low complexity and low power consumption WSNs are vulnerable to Distributed Denial-of-Service (DDoS) attacks due to its broadcast nature of communication and limited power supply**.** Hence security and energy efficiency are the two important challenging tasks in WSN. In this paper, Energy Efficient Intrusion Detection System (EE-IDS) has been proposed for IEEE802.15.4 based WSN to detect and mitigate the Distributed Denial of Service (DDoS) attack (resource depletion, power exhaustion attacks and flooding). The design of EE-IDS includes optimized watchdog system and Hidden Markov Model (HMM). The proposed EE-IDS and existing Energy Efficient Trust System (EE-TS) are simulated and compared by using Ns2 simulator. The simulation results depict that EE-IDS has better performance in terms of Packet Delivery Ratio (PDR), average end-to-end delay, packet drop and energy consumption of network than that of EE-TS.

Index Terms: Intrusion detection system, Wireless sensor networks, Watchdog approach, DDoS attacks, Hidden markov model.

1. INTRODUCTION

In many WSN applications, security is an essential concern especially for the application designed using IEEE 802.15.4 based WSNs deployed in hostile environments and commercial applications. Even though, security solutions like authentication, cryptography or key management techniques enhance the WSNs security, they cannot prevent all possible DDoS attacks such as resource depletion attacks, power exhaustion attacks and flooding attacks. One practical security defense scheme namely Intrusion Detection System (IDS) [1] is needed for the detection of all types of attacks, because traditional cryptography-based security mechanisms such as authentication and authorization are not effective against such attacks.

In the recent years many IDSs have been proposed for wireless sensor network. Among the existing IDS, a trust based watchdog approach [3] is an effective mechanism for DDoS attacks.

The watchdog technique is a trust based intrusion detection technique which identifies the malicious nodes and its activity in the network is to monitor the nodes within its communication range. The nodes selected as the watchdog nodes 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. 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 also the intermediate node, can determine whether the data packet is being properly transmitted by the intermediate node. Thus the watchdog node checking the validity of the nodes involved in the transmission of the data packet.

* Department of Electronics Engineering, Pondicherry University, Puducherry-14, India, *E-mail: jeganece84@gmail.com*

** Department of Electronics Engineering, Pondicherry University, Puducherry-14, India, *E-mail: samundiswary_pdy@yahoo.com*

This is due to the fact that, when the source node forwards it's packets 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 all 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. Most existing works mainly focus on the design of the trust models and how these models can be used to defend against certain DDoS attacks [4]. Basically, DOS attacks can be categorized into three types. They are a) Consumption of scarce, limited or non-renewable resources. b) Destruction or alteration of configuration information. c) Physical destruction or alteration of network resources. If a network consists of multiple DOS attacks at a time, which may leads to DDOS attacks. In context of WSN, the DDoS attacks destructive to networks are resource depletion, power exhaustion and flooding attack. In this paper, a novel approach for implementing EE-IDS to detect the DDoS attacks in IEEE 802.15.4 based WSN is proposed. The design of EE-IDS comprises of optimized watchdog system and Hidden Markov Model (HMM). The optimized watchdog mechanism is a trust based method which is used to evaluate the trustworthiness of the network. The DDoS attack is detected based on energy consumed using the Hidden Markov Model. The rest of this paper is organized as follows. Section 2 describes the literature review and section 3 deals with the proposed IDS for detection of DDoS attacks using Optimized Watchdog System. Section 4 discusses about the simulation results and finally section 5 concludes the paper based on findings and analysis.

2. LITERATURE REVIEW

C. Balarengadurai et al [4] 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 using the Fuzzy Based Detection and Prediction System (FBDPS), any node consuming huge amount of energy is detected as a malicious node. Based on the rate of energy consumed by the node, FBDPS differentiates the kind of the DDoS attack.

Bernardo M. David et al [5] 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. This trust model can be accordingly adopted and applied in different protocols and networks.

Anthony D. Wood et al [6] have proposed Defeating Energy-Efficient JAMming (DEEJAM), a new MAC-layer protocol for identifying the hidden jammers with IEEE 802.15.4-based hardware. It uses four techniques to protect the data transmission from the attacking jammer, escapes its attack and minimizes its effect. This protocol effectively overcomes many complicated and dangerous attacks such as interrupt jamming, activity jamming, scan jamming, and pulse jamming.

Among the existing works based on watchdog, the security vulnerabilities of some of the watchdog and trust mechanisms and counter measures are discussed in the paper [7].

Forootaninia et al [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 cost 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.

3. DETECTION OF DDOS ATTACKS USING OPTIMIZED WATCHDOG SYSTEM

3.1. Overview

In this paper, the optimized watchdog trust system [9] for detecting the DDoS attacks has been extended. Here each watchdog node estimates the trustworthiness of node by collecting the hop by hop queuing delay and received traffic. A topology discovery phase is conducted by the sink node such that the routing path from each node to the sink is stored in the respective nodes.

The DDoS attack includes resource depletion attack, battery exhaustion attack and flooding attack. For these attacks, energy dissipation rate of sensors is predicted by applying the Hidden Markov Model (HMM)[10]. The watchdogs collect the residual energies from the monitored nodes. It estimates the actual energy consumed from the reported residual energies and compares them with predicted energy values. The nodes with abnormal energy consumption are considered to be malicious nodes. Figure 1 illustrates the functional flow diagram of the proposed system.

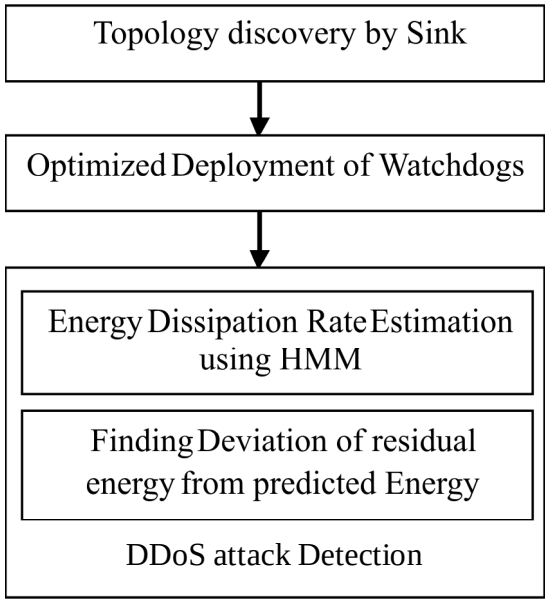

Figure 1: Functional flow diagram of proposed system

3.2. 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 neighbor 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 neighbor node ID, residual energy (E_R), Queue Delay (QD) of each node along with the 2-hop neighborhood information.

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. By utilizing the updated node information, the topology is discovered by 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 2, 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 $d_{ij} \le r_i$ and $d_{ij} \le r_j$. Let $B_i = \{n_j \mid e_{ij} \in N\} = \{nj \mid dij \le ri \;\&\; d_{ij} \le r_j\}$, $B_i \in N$ 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., $d_{23} \le r_2$ and $d_{24} \le r_2$) 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 accuracy and trust robustness. 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 perform watchdog task and to schedule watchdog tasks among those selected watchdog nodes.

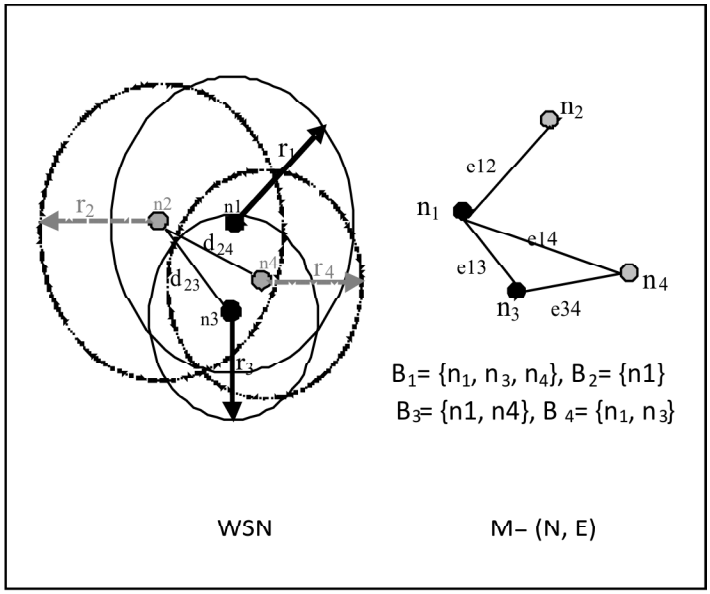

Figure 2: A WSN and the system model M

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_j. The node n_i can work as a watchdog to monitor only $\forall\, n_j \in B_i$, and vice versa, only $\forall\, n_j \in B_i$ can perform watchdog tasks to monitor n_i. The nodes that are located close to the optimal d_{ij} must be selected as watchdog nodes. 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.

3.4. Detection of the Distributed Denial of Service (DDoS) attack

The malicious nodes have to use additional energy to launch DDoS attacks in MAC layer [12]-[15]. Therefore, the prediction of energy consumption at various states of sensor node, to predict the malicious nodes is proposed. For this, energy dissipation rate of sensors is predicted by applying the Hidden Markov Model (HMM).

3.4.1. Energy Estimation using Hidden Markov Model (HMM)

The HMM is an extension of the conventional Markov Model. In HMM, the Markov process is not visible i.e., it is hidden and only the final result of the process can be seen. Only the final state is observable in HMM. There are different states in HMM like the initial state, transition state and observed state. Every state has a probability distribution on the different possible outcomes. The sequence followed by the process is hidden but not the result i.e., observed state.

HMM includes the set of hidden states (*S*) and set of observation states (*V*). The basic picturization of HMM is shown in figure-3.

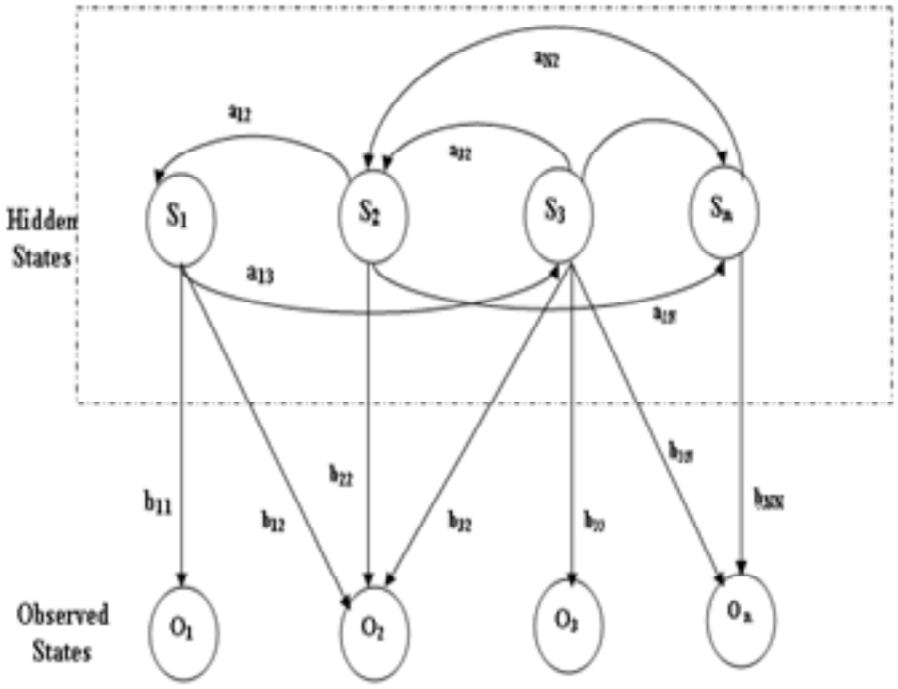

Figure 3: Hidden Markov Model (HMM)

The set of hidden and observation states are represented below in equation (1) and (2) respectively

$$S = (s_1, s_2, s_3, ..., s_n) \tag{1}$$

$$V = (v_1, v_2, v_3, ..., v_m) \tag{2}$$

Let *Q* be the state sequence of fixed length *L*, to corresponding observations *O*,

$$Q = q_1, q_2, q_{3,...,} q_L \tag{3}$$

$$O = o_1, o_2, o_3, ...o_L \tag{4}$$

HMM is generally formulated as,

$$\lambda = (A, B, \pi) \tag{5}$$

In the equation (5), *A* denotes the transition array, which is independent of time *t* and keeps track of probability of interference state *j* following interference state *i* and indicated as below,

$$A = \left[a_{ij} \right], a_{ij} = P\left(q_t = s_j \mid q_{t-1} = s_i \right) \tag{6}$$

Whereas, array of observation is represented by *B* and it is independent of time *t*. It stores the probability of observation *k*, which is produced from the state *j*. The observation array *B* is detailed in equation (7)

$$B = \left[b_i \left(k \right) \right], b_i \left(k \right) = P \left(x_t = v_k \mid q_t = s_i \right) \tag{7}$$

π signifies the initial state probability as shown below,

$$\pi = \left[\pi_i \right], \pi_i = P \left(n_1 = I_i \right) \tag{8}$$

In this paper, the observation states correspond to the power consumed during various states of a sensor node, namely, TRANSMIT, RECEIVE, PROCESS and IDLE.

(ie)

$$O = \{TxP_1, RxP_1, PrP_1, IP_1,$$
$$TxP_2, RxP_2, PrP_2, IP_2,$$
$$.....$$
$$.....$$
$$TxP_n, RxP_n, PrP_n, IP_n\}$$

where *TxP*, *RxP*, *PrP* and *IP* denotes transmit power, receive power, processing power and idle power, respectively at *n* time intervals. The output (hidden state) will be the cumulative energy dissipation rate of the corresponding nodes over the n time intervals.

3.4.2. DDoS Attack Detection Algorithm

The detection of the DDoS attack is based on the HMM scheme for the estimation of the energy consumption [11]. The algorithm for detection of the DDoS attack described below.

Notations:

- $E_{consumed}$: 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 based on $E_{consumed}$

Algorithm:

- Watchdog node estimates $E_{consumed}$ using HMM filter as described in section 3.4.1
- The watchdog also collects the residual energy ($E_{collected\_residual}$) from all the monitored nodes.
- Watchdog estimates the difference between the initial energy and $E_{consumed}$, to calculate the $E_{calculated\_residual}$
- Then the watchdog compares the calculated residual energy ($E_{calculated\_residual}$) with the $E_{collected\_residual}$
- If $E_{collected\_residual} = E_{calculated\_residual}$, then energy consumed is normal
  - If $E_{collected\_residual} \neq E_{calculated\_residual}$, then energy consumed is abnormal
- If there is a huge difference during comparison, this indicates abnormal consumption of energy by the node.
- If the huge difference in the energy consumption level depicted by the watchdog and the HMM technique get matches. Then, this indicates that the node is malicious and the occurrence of the DDoS attack.
- Thus, the DDoS attack is efficiently detected in the network.

4. SIMULATION RESULTS

4.1. Simulation Parameters

The proposed and existing system is evaluated by using NS2 simulator [16]. IEEE 802.15.4 is used as the MAC layer protocol. The performance parameters such as packet delivery ratio, average end-to-end delay, packets drop and energy consumption has been evaluated and compared with the existing EE-TS. In the simulation, the number of attacker is varied as 1, 2, 3, 4 and 5. The simulation settings and parameters are summarized in table 2. Figure 4 illustrates the wireless sensor network scenario, which consists of 101 nodes deployed over a terrain with size 100×100 m^2 with DDoS attacks in MAC layer.

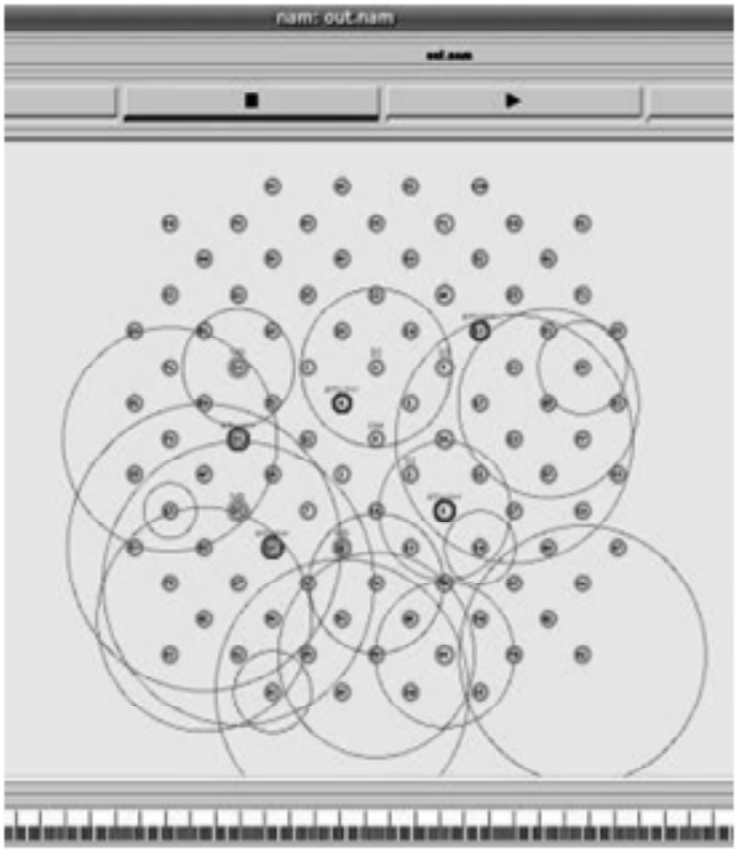

Figure 4: WSN Scenario with DDoS Attack

4.2. Results & Analysis

The descriptions of simulated results are presented in this section. Fig.5 and 6 shows the effect of packet delivery ratio w.r.t DDoS attacks and data rate for existing and proposed system. It is inferred through the figures that proposed EE-IDS outperforms Existing Energy Efficient Trust System (EE-TS) by 8% in terms of Packet delivery ratio. The outperformance of proposed EE-TS is due to the detection and termination of network link with attacks as soon as intruder occurs in the network. Figure-7 and 8 shows the effect of packets drop with respect to DDoS attacks and data rate for existing and proposed system. The results portrayed in figure-7 and figure-8 illustrate that proposed EE-IDS outperforms Existing Energy Efficient Trust System (EE-TS) by 19% and 17 % in terms of packets drop.

Table 2
Simulation parameters

No. of Nodes	101
Area	100×100 m^2
MAC	IEEE 802.15.4
Routing Protocol	AODV
Simulation Time	60 sec
Traffic Source	Poisson
Attackers	1, 2, 3, 4 and 5
Propagation	Two Ray Ground
Antenna	Omni Antenna

Figure 9 and 10 illustrates the variation of energy consumption of networks with respect to increased DDoS attacks and data rate for existing and proposed system. The results depict that proposed EE-IDS outperforms EE-TS by 4% in terms of Energy consumption.

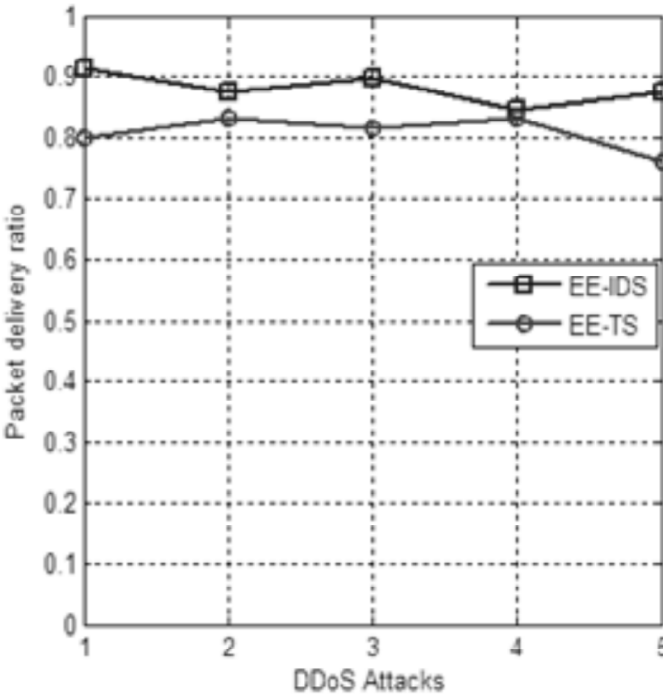

Figure 5: Packet Delivery Ratio Vs DDoS Attacks (Data rate= 150 Kbps)

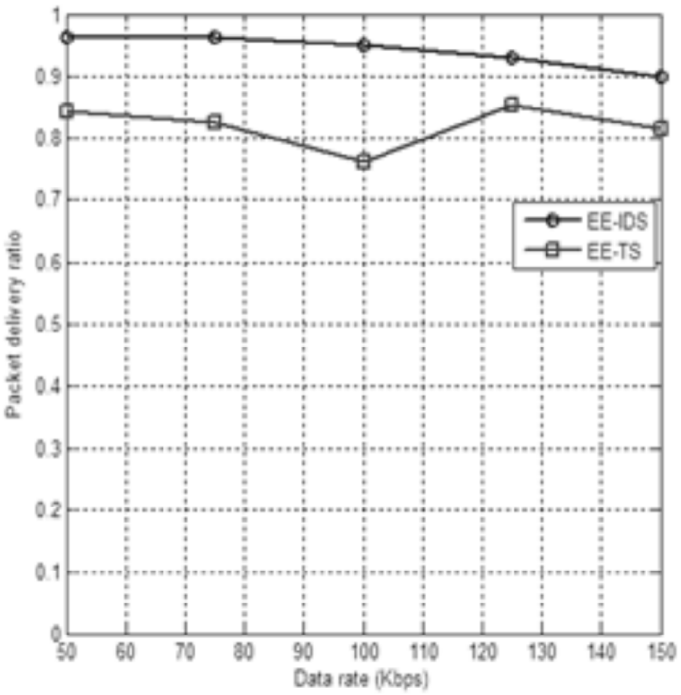

Figure 6: Packet Delivery Ratio Vs Data rate (With 3 DDoS attacks)

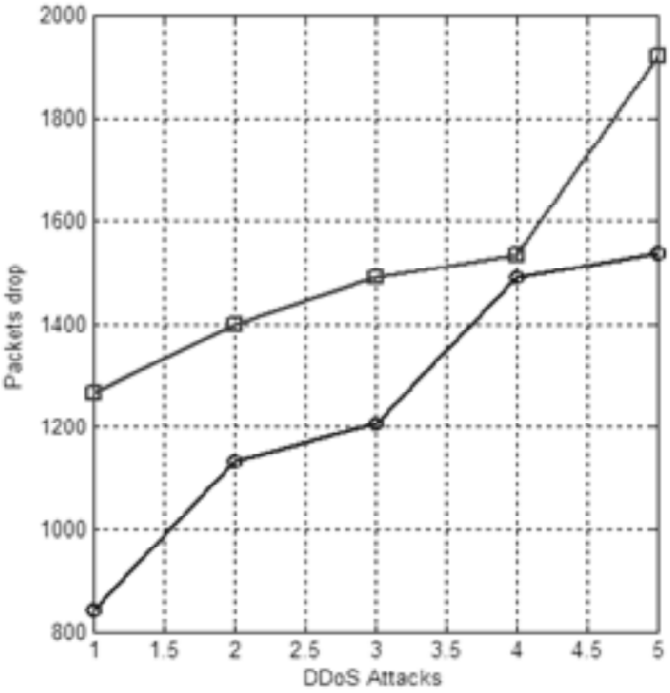

Figure 7: Packets Drop Vs DDoS Attacks (Data rate=150kbps)

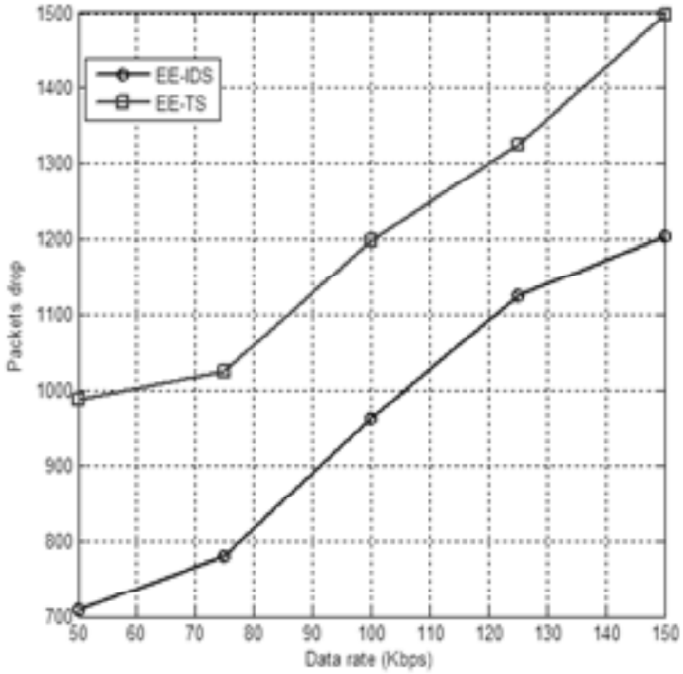

Figure 8: Packets Drop Vs Data Rate (With 3 attacks)

The effect of average end-to-end delay w.r.t DDoS attacks and data rate is shown in figure11 and 12. It is observed that average end-to-end delay is increases with increased number of DDoS attacks, and decreases w.r.t data rate for both the system. However the proposed EE-IDS is having higher average end-to-end delay compared to that of existing EE-TS.

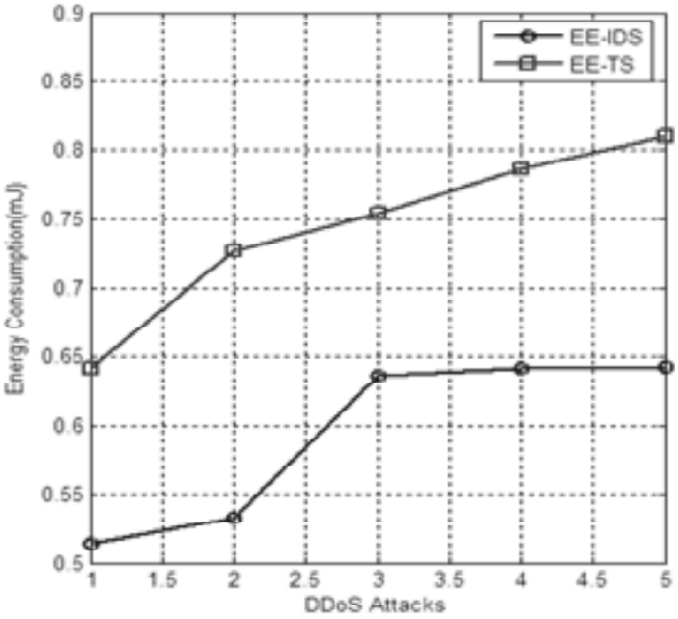

Figure 9: Energy Consumption Vs DDoS Attacks (Data rate= 150 Kbps)

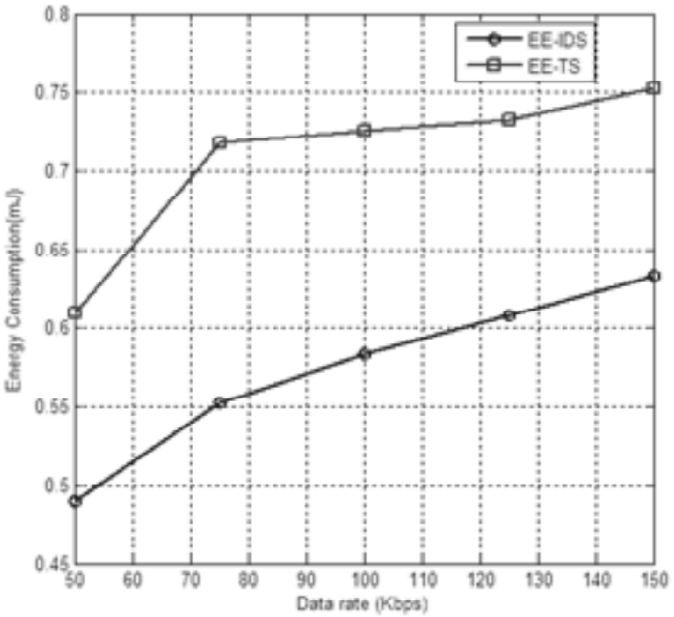

Figure 10: Energy Consumption Vs Data rate (With 3 attacks)

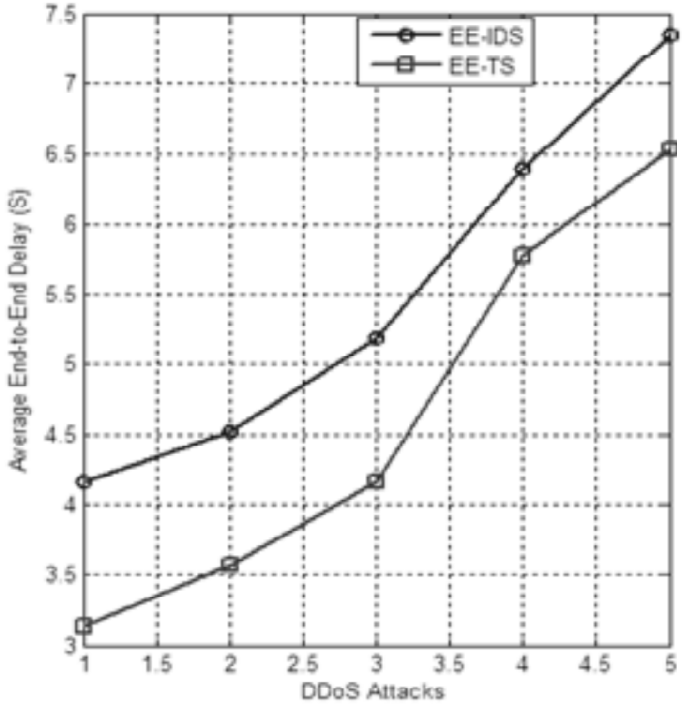

Figure 11: Average end-to-end delay Vs DDoS Attacks (Data rate= 150 Kbps)

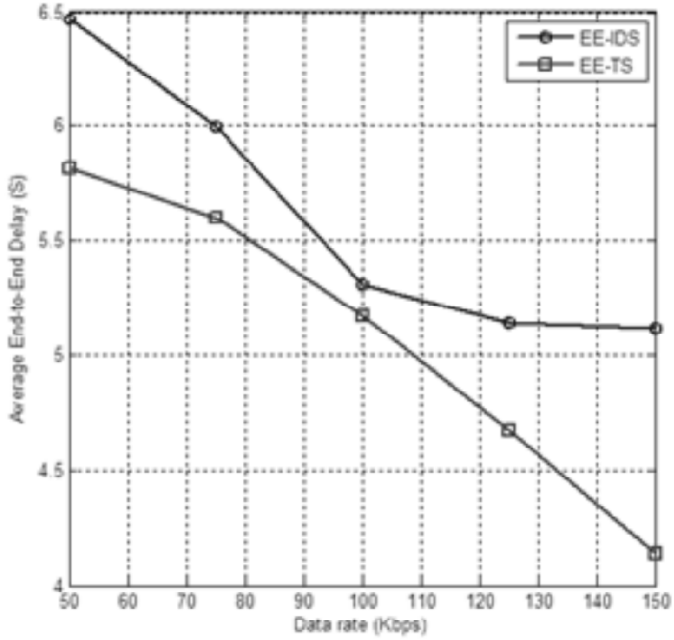

Figure 12: Average end-to-end delay Vs Data rate (With 3 attacks)

5. CONCLUSION

In this paper, the EE-IDS using optimized watchdog system with HMM technique for detecting DDoS attacks in IEEE 802.15.4 based WSN is developed. The simulation is done by using NS-2 simulator. It is proved through the simulation results that EE-IDS has better performance than that of EE-TS in terms of packet delivery ratio, packets drop and energy consumption. Further the work can be extended by incorporating security algorithm for detecting network layer attacks in IEEE 802.15.4 based WSN.

References

[1] Abror Abduvaliyev, 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.

[2] Murad A. Rassam, Anazida Zainal and Mohd Aizaini Maarof, "Advancements of Data Anomaly Detection Research in Wireless Sensor Networks: A Survey and Open Issues", *Sensors*, pp. 10087-10122, 2013.

[3] Youngho Cho and Gang Qu "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.

[4] 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.

[5] 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.

[6] 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* (SECON'07), pp. 60-69, June 2007.

[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*, pp. 134-141, 2012.

[8] 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.

[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*, vol. 10, no. 3, pp. 613-625, March 2015.

[10] Lawrence rabiner "A tutorial on hidden markov models and selected applications in speech recognition", *Proceedings of the IEEE*, vol. 77, no. 2, pp- 257 – 286, 1989.

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

[12] Radosveta Sokullu, Ilker Korkmazy, Orhan Dagdevirenz, Anelia Mitsevax, Neeli R.Prasad, "An Investigation on IEEE 802.15.4 MAC Layer Attacks", *Proc. of Wireless Personal Media Communications* 2007.

[13] Radosveta Sokullu, Ilker Korkmazy, Orhan Dagdevirenz, Anelia Mitsevax, Neeli R.Prasad, "An Investigation on IEEE 802.15.4 MAC Layer Attacks", *Proc. of Wireless Personal Media Communications* 2007.

[14] 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, pp. 253-271, 2010.

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

[16] Network Simulator: http:///www.isi.edu/nsnam/ns