International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 8 (2017) pp. 1772-1778

Design of Hierarchical Trust based Intrusion Detection System for Wireless Sensor Network [HTBID]

Amol R. Dhakne[1]*, and Prashant N. Chatur[2]

[1,2]Department of Computer Science and Engineering,
Government College of Engineering, Amravati-444601, India.

Abstract

In this paper, a Hierarchical Trust based Intrusion detection System [HTBID] has been proposed to effectively deal with various attacks in wireless sensor network. HTBID deals with different types of attack with the help of Hierarchical Trust evaluation protocol [HTEP]. This work identifies different parameters and factors that affect trust of wireless sensor network. HTEP considers attributes derived from communication as well as social trust to calculate the overall trust of sensor node. Our results indicate that HTBID gives better results in terms of detection rate, false positive rate, packet delivery ratio, etc., for different types of attack in wireless sensor network.

Keywords: Wireless Sensor Network, Intrusion Detection, Peer-to-peer Trust, Trust Evaluation, Selective Forwarding Attack, Blackhole Attack, OnOff Attack.

INTRODUCTION

Wireless Sensor Network is evolving technology where small nodes are deployed in open environment to sense various phenomenon's such as temperature, pressure, pollutants or motions, etc. Also WSNs can be used for the purpose of monitoring the environment for battlefield surveillance, weather or wild animals. As these sensor nodes are limited by resources and are deployed in open environment, these nodes are always prone to different types of attacks either inside attacks or outside attack. Security mechanism such as cryptography techniques provide the security services to ensure authenticity, integrity and confidentiality of transmitted data, but these techniques does not deal with outside attacks such as sinkhole attack, blackhole attack or denial of service attack etc., To deal with these attacks researchers propose trust models [1]. Trust management have been successful in other areas of networks such as ad hoc network, social network and p2p network. But methods and mechanisms that are applicable to other networks are not directly applicable to wireless sensor network as these are limited by resources.

Trust in wireless sensor network can be viewed in terms of communication trust, data trust, path trust, node trust or service trust. Trust can be defined as subjective opinion of other entity in terms of processing capability or availability of service. Trust is reflexive, non-transitive, subjective and asymmetric in nature. If node performs according the rules and regulations of networking, then trust between nodes increases. If node does not perform according to the rules of networking the trust between node decreases and node must be considered as malicious one. Such nodes need to be eliminated from further communication in network [2].

In this work, a hierarchical trust based intrusion detection system is proposed to deal with various attacks [3] in wireless sensor network. Key design issues including composition, aggregation and formation of trust management have been addressed.

Paper is organized in following manner. Section II describes the system model. Section III describes Hierarchical Trust Evaluation Protocol [HTEP] for hierarchically structured or Cluster based WSN. In section 4 we apply our Hierarchical trust evaluation algorithm for purpose of intrusion detection in wireless sensor network considering different attacks. Section 5 shows the results of simulation for our HTBID. Finally section 6 concludes the paper.

SYSTEM MODEL

Here we consider Cluster based WSN as it is much easier to manage cluster head (CH) from every cluster than managing each and every sensor node in whole network.

Sensor nodes in WSN have many limitations in terms of energy, transmission power, storage and computing capability. Most of energy of sensor node is consumed by sensor nodes for communicating the data from sensor node to base station and it causes the energy depletion in sensor nodes.

There are different advantages of Clustering in wireless sensor network.

1) It helps to reuse bandwidth and improves the capacity of system to perform more networking function.
2) Energy is saved as all sensor nodes send their data to CHs and it helps to reduce multiple routes and loops of routing.
3) As Clustering allocates resources properly, it helps in better design of power control.
4) Any change made within a cluster, does not affect entire network and therefore network becomes robust to such changes.

Cluster head (CH) can be selected by using protocol such as Hybrid Energy Efficient Distributed Clustering (HEED) [4]. Sensor node sends their data to CH by using sensor nodes within cluster and then CH sends data to base station or destination node.

By considering the benefits of two level hierarchies in WSN, our Trust Evaluation Protocol is conducted for the peer to peer trust calculation between two SNs and two CHs. Our protocol is conducted at two levels. At SN node level, sensor node calculates peer-to-peer trust of other sensor node within its cluster and reports results to CH where each cluster head again evaluates the CH-to-SN trust of each sensor node within its cluster.

Similarly, at CH level, Cluster head calculates the peer-to-peer trust of other CHs and reports result to Base station (BS). Base station calculates the BS-to-CH trust for all cluster Heads (CHs) in network system.

In section 3, we will describe the Hierarchical Trust Evaluation Protocol [HTEP] to calculate the Peer-to-peer trust, CH-to-SN and BS-to-CH trust.We consider both aspect of trustworthiness such as social trust and QoS trust to form composition of our trust metric. Social trust can include the various parameters such as honesty, privacy, intimacy, connectivity and centrality. QoS can include parameters such as cooperativeness, task completion capability, competence, reliability etc. Our trust evaluation protocol is formulated in such a manner that it combines both trusts metric to form overall trust.

In this protocol we consider energy and unselfishness to measure QoS trust derived from communication network. Energy is used to measure the competence. It is very important metric as sensor nodes are energy constrained. It is used to decide whether particular node is competent enough to carry out given task. Unselfishness is used to measure the cooperativeness. We select the intimacy and honesty to measure the social trust which will be derived from social network. Intimacy is used to measure the closeness between nodes based on past interaction experiences. Maturity model proposed in [5] can be used to measure intimacy between nodes based on past interaction. Honesty is used for measuring the regularity and also it implies about maliciousness of node.

Our trust evaluation protocol can be applied to heterogeneous WSN where each sensor node can have different energy and different degree of selfishness or maliciousness. SN can become selfish when it has low energy or it has a lot of unselfish neighbour nodes. SN can become compromised when it is surrounded by more compromised nodes. CH is likely to consume more energy than sensor nodes. If SN or CH gets compromised it may consume more energy to perform different types of attack. As opposed to compromised nodes, the selfish node consumes less energy than unselfish nodes, as they behave to stop sensing functions and they drop messages arbitrarily.

Different types of attacks are performed by compromised node including selective forwarding attack, forgery attack, Sybil attack, denial-of-service attack, black hole/sinkhole attack. If some of these attacks are performed successfully, they can make system fail. Thus it is important to detect the attacks quickly and evict them before system failure can occur.

In this paper we show that our Hierarchical trust evaluation protocol is resilient to Selective forwarding attack, Blackhole attack and ONOFF attack[3] as compared with other trust model.

HIERARCHICAL TRUST EVALUATION PROTOCOL [HTEP]

Illustrations Firstly we describe hierarchical trust evaluation algorithm addressing the issues of formation of trust, aggregation of trust and composition of trust. After that we will apply this to cluster based WSN described in system model.

Our Hierarchical trust Evaluation Algorithm maintains two level of trust: SN level trust and CH level trust. Each SN evaluates the trust of other sensor node in the same cluster whereas each CH evaluates the trust of other CH and sensor nodes in its cluster. Peer-to-peer trust is evaluated based on either direct observations or indirect observations. If nodes are neighbours of each other within their radio range then they evaluate trust based on direct observations through overhearing or snooping. Every sensor node sends the results of trust evaluation about other SNs in same cluster to its CH. Every CH evaluates the trust of SNs within its cluster. Similarly, every CH sends the result of trust evaluation about other CHs in Same WSN to CH Commander which is residing on base station. If base station is not available then it sends evaluation results to elected CH. CH commander evaluate the trust of all CHs in WSN. Election protocol such as HEED [4] can be used for election of CH commander which is not the scope of this paper.

Four different types of trust components intimacy, honesty, energy and unselfishness are considered while calculation of these two levels of peer-to-peer trust. Trust value that node(a) evaluates towards node(b) at time t, T_{ab} (t), is represented in the form of real number in range of [0, 1] where 0 indicates no any trust, 0.5 ignorance and 1 complete trust. T_{ab} (t) is calculated by :

$$T_{ab}(t) = w_1 T_{ab}^{intimacy}(t) + w_2 T_{ab}^{honesty}(t) + w_1 T_{ab}^{energy}(t) + w_1 T_{ab}^{unselfishness}(t) \quad (1)$$

Where w_1, w_2, w_3 and w_4 are the weights associated with trust components intimacy, honesty, energy, unselfishness respectively in such a way that $w_1 + w_2 + w_3 + w_4 = 1$. We have to decide best values for weights so as to maximize the performance of application which is trust formation issue.

Peer - to - Peer Trust Evaluation :

Here we show how two peer SNs or two peer CHs evaluate Peer –to – peer trust among them. When a trustor node (a) evaluates trustee node(b) at time t, it updates T_{ab}^{X} (t) where X is a component of trust indicated as follows:

$$T_{ab}^{x}(t) = \begin{cases} (1-\alpha)T_{ab}^{x}(t-\Delta t) + \alpha T_{ab}^{X,direct}(t), \\ if\ a\ and\ b\ are\ 1-hop\ neighbors; \\ avg_{k\in N_a}\{(1-\gamma)T_{ab}^{x}(t-\Delta t) + \gamma T_{kb}^{X,recom}(t), \\ otherwise. \end{cases} \quad (2)$$

Above equation 2 conclude that if node node a is 1-hop neighbour of node b, then node a will compute new trust based on the direct observations ($T_{ab}^{X,direct}(t)$) and old trust based on past experiences ($T_{ab}^{x}(t-\Delta t)$) where Δt is the interval of trust updating toward node b to update $T_{ab}^{x}(t)$. A parameter α is used to assign weights to old trust value and new trust value ranging from 0 to 1. It is also useful for considering the decay over time i.e., we should consider trust value decay and new trust value contribution. If value of α is large then it means that trust evaluation is more relying on direct observations. Here $T_{ab}^{X,direct}(t)$ indicates the trust value of node a toward node b based on direct observations evaluated over period of time [0, t]. Following section describes how these direct trust component values can be obtained when node a and b are 1-hop neighbours:

$T_{ab}^{intimacy,direct}(t)$: It is used to measure the interaction experiences among nodes. It is calculated based on total number of interaction among node a and b over total total number of interaction among node a and any other neighbour node over period of time [0,t]. [6]

$T_{ab}^{honesty,direct}(t)$: This component refers to the belief of node a that node b is honest based on direct observations of node a toward node b. To evaluate $T_{ab}^{honesty,direct}(t)$, count of suspicious dishonest experience about node j observed during time period [0,t] are used. Set of anomaly detection rules such as interval, retransmission, delay, repetition and high discrepancy rules in sensor reading or recommendation are used to keep track of dishonest experiences. [7], [8]. $When\ T_{ab}^{honesty,direct}(t)$ = 0, i.e. when count of dishonest experiences exceeds system defined threshold, then node b is considered as dishonest at timr t . Otherwise, it is computed by 1 minus ratio of count to threshold. Generally, dishonest behaviour is shown by compromised nodes

$T_{ab}^{energy,direct}(t)$: It is the belief of node a that node j still have required energy to carry out intended networking function. It is symbol to measure competence of node. Percentage of remaining energy of node b can be used for this computation. Energy consumption models described in [9] – [11] can be used to calculate the remaining energy of node j by overhearing node b's activities of packet transmission over time period [0, t].

$T_{ab}^{unselfishness,direct}(t)$: It represents intent of unselfishness of node b evaluated by node a based on direct observation over period of time [0, t]. Snooping and overhearing techniques can be used by node a to identify the selfish behaviours of node b such as not performing functions of sensing, forwarding and reporting [12], or not executing the trust management protocol as prescribed. Latest interaction experiences can be given high priority than old experiences while evaluating $T_{ab}^{unselfishness,direct}(t)$. Generally, it is considered that compromised nodes are not cooperative and thus treated as selfish.

By considering the other side if node a is not a 1-hop neighbour of node b then it will evaluate node b based on past experience $T_{ab}^{x}(t-\Delta t)$ and recommendations from its 1-hop neighbours $T_{kb}^{X,recom}(t)$ to evaluate $T_{ab}^{X}(t)$,where k is recommender. for the purpose of scalability and energy conservation, only 1 – hop neighbours (N_a) will be used by node a as a recommender. If N_a is empty set i.e., if there is no any neighbour of node a, then a is orphan, where $\gamma = 0$, thus peer-to-peer trust evaluation is not possible through node a. Parameter γ is used to assign weights to recommendations, past experiences and consider trust decay over time as given in equation 3.

$$\gamma = \frac{\beta T_{ak}(t)}{1+\beta T_{ak}(t)} \quad (3)$$

Here parameter $\beta \geq 0$ is used for specifying the impact of "indirect recommendations" on evaluation of trust in such a manner that indirect recommendation weight is normalised to $\beta T_{ak}(t)$ instead of 1 assigned to past experiences. As β or $T_{ak}(t)$ is increased the contribution from recommended trust increases proportionally.

CH-to-SN Trust Evaluation :

Every SN reports the result of trust evaluation about other node within same cluster to CH. CH then performs CH-to-SN trust evaluation toward node b by applying the statistical analysis method (as in equation 4) by using $T_{ab}(t)$ values received as result of peer-to-peer trust evaluation of nodes.

The values of $T_{ab}(t)$ can be used to detect if there is any evidence of good mouthing or bad mouthing attack. Based on CH-to-SN trust evaluation result toward node b d, CH determines whether node b is trustworthy or not, and whether node b should be excluded from sensor reading and routing duties. CH, c, performs intrusion detection while evaluating SN b by comparing trust value of node b $T_{cb}(t)$ with minimum trust threshold of system $T^{th.}$ Value of $T_{cb}(t)$ is evaluated by following equation 4.

$$T_{cb}(t) = avg_{a\in M_c\ \lambda\ T_{ca}(t)\geq T^{th}}\{T_{ab}(t)\} \quad (4)$$

Where M_c indicates the set of SN in the cluster. If value of $T_{cb}(t)$ is less than T^{th} then node b will be announced as compromised by CH c; otherwise node b is not considered as compromised. Here values of trust are collected from nodes which are considered as trustworthy by CH. That is trust recommendation will be taken from node (a) only when $T_{ca}(t) \geq T^{th}$. In section IV, a methodology to implement trust based intrusion detection is described as application of Hierarchical trust Evaluation Protocol.

Station-to-CH Trust Evaluation :

One hop radio range of CH is larger than those of SNs as capacity and transmission power of CH is higher than SNs. CH gathers and aggregates the sensor readings to forward information hop-by-hop through other CHs to base station. It makes a lot of interaction among two neighbour cluster heads CHs similar to two SNs in same cluster. CH-to-CH trust evaluation is carried out in same manner of SN-to-SN trust evaluation as described in section IV (a) Every CH reports results of trust evaluation about other CHs to base station which is physically more protected. CH commander which resides on base station performs the same statistical analysis as in equation 4 to T_{ab} (t) values received from all CHs in system to perform station-to-CH trust evaluation towards CH b. After the analysis, base station decides about status of CH, whether CH is compromised or not so as to exclude it from CH and routing duties.

HIERARCHICAL TRUST BASED INTRUSION DETECTION [HTBID]

As nodes in WSN are deployed in open environment, they are more vulnerable to different types of attack. There have been different types of Intrusion detection systems such as anomaly based IDS, Specification based IDS, Game theory based IDS proposed for WSN etc., [13]. This section describes how Hierarchical Trust Based Intrusion Detection HTBID can be used by CH (or base station) to perform intrusion detection of SNs (or CHs) under their control. We apply our hierarchical trust evaluation protocol [HTEP] to intrusion detection as an application.

We conduct the simulation for three different types of attack in wireless sensor network such as Black hole attack, selective forwarding attack and ON OFF attack. Black hole attack is one which drops all packets that have been sent by neighbour node for further transfer. A selective forwarding attack is one where node forwards only selected packets to sink node with some probability p and drops other packets. ONOFF attack is the one where node initially behaves well to achieve the high trust value and then drops packet when attacker mode is in ON state and forwards packet when attacker mode is in OFF state. Following section shows simulation

SIMULATION RESULTS AND COMPARISON

Intrusions can be detected by this Hierarchical Trust based Intrusion Detection System [HTBID] in wireless sensor network which can run on CH or base station. This system uses Hierarchical Trust Evaluation protocol [HTEP] which has been described in section 4. Simulations have been conducted in ns2. To simulate our method we use the 50 wireless sensor nodes and the simulation area is considered as 950*950. Simulation setup settings and other assumptions are as follows.

TABLE 1. SIMULATION SETUP PARAMETERS

Parameters	Values
Simulator	Network Simulator 2
Number of Nodes	50
Interface Type	Phy/Wirelessphy
Channel	Wireless Channel
Mac Type	Mac/802_11
Queue Type	Queue/Droptail/Priqueue
Queue Length	201 Packets
Antenna Type	Omni Antenna
Propagation Type	Two ray Ground
Size Of Packet	Five Hundred And Twelve
Traffic	Tcp

We have compared performance of Hierarchical Trust based Intrusion Detection [HTBID] with Efficient Distributed Trust model (EDTM) [14] in Wireless Sensor Network. Comparison have been done by considering the different parameters in presence of three types of attacks such as Selective forwarding attack, Blackhole attack and ONOFF attack. Different parameters considered for comparison are false positive rate, packet delivery ratio and Detection rate.

In Figure 1. system model for Cluster based WSN have been depicted. Nodes that have highest energy are selected as CH in WSN. Base station performs HTBID on all cluster head and CH performs HTBID on SNs in its cluster.

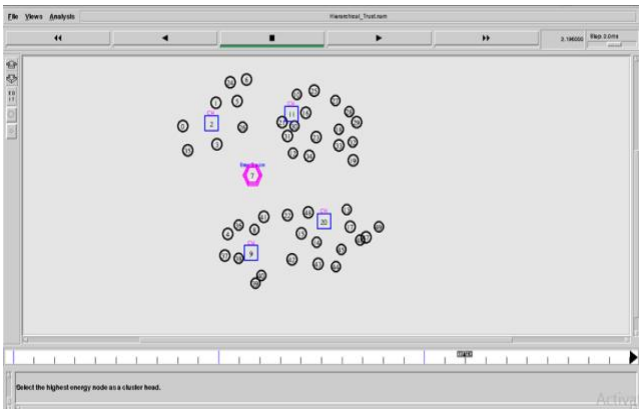

Figure1. System model for Cluster based WSN

Simulation have been conducted in presence of three types of attack such as selective forwarding attack, blackhole attack and ONOFF attack. Figure 2. Shows that false positive rate of HTBID system is less than EDTM model in presence of selective forwarding attack.

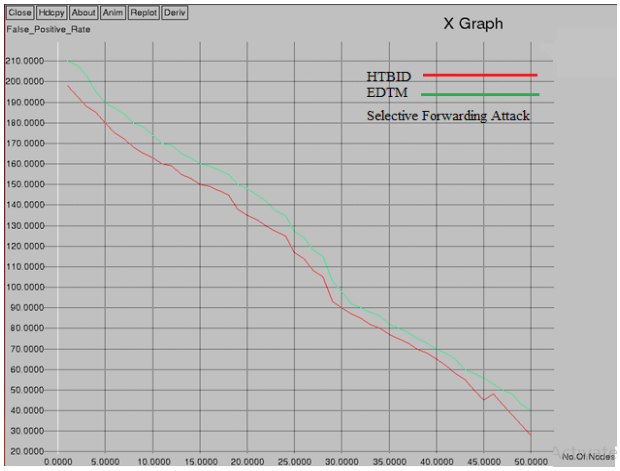

Figure 2. False positive rate in presence of Selective forwarding attack

Figure 3, shows that Packet delivery ratio (PDR) of HTBID is higher than EDTM in presence of selective forwarding attack.

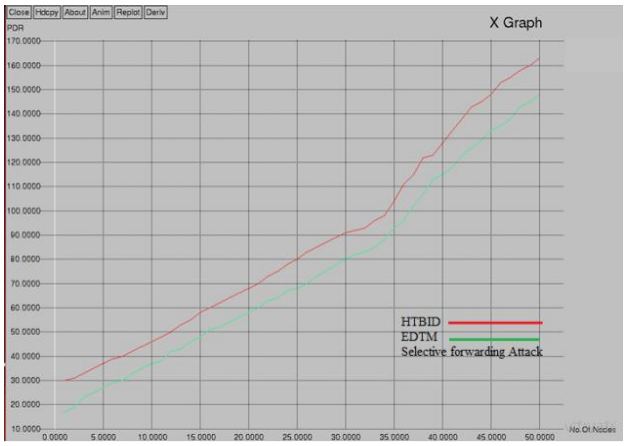

Figure 3. PDR in presence of Selective forwarding attack

Figure 4, shows that detection rate of HTBID is more than EDTM in presence of selective forwarding attack.

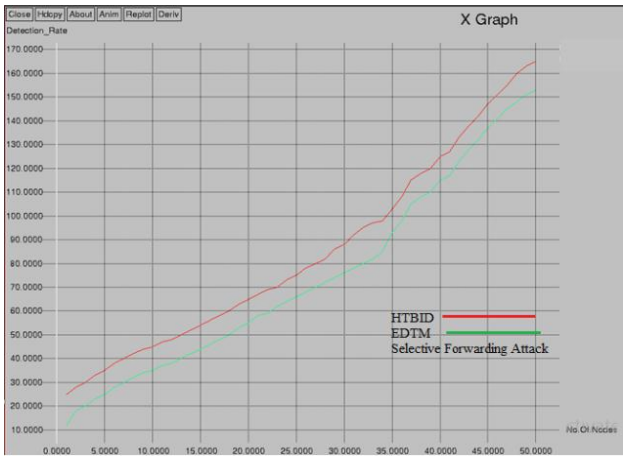

Figure 4. Detection rate for Selective Forwarding attack

Figure 5. Shows that false positive rate of HTBID system is less than EDTM model in presence of Blackhole attack.

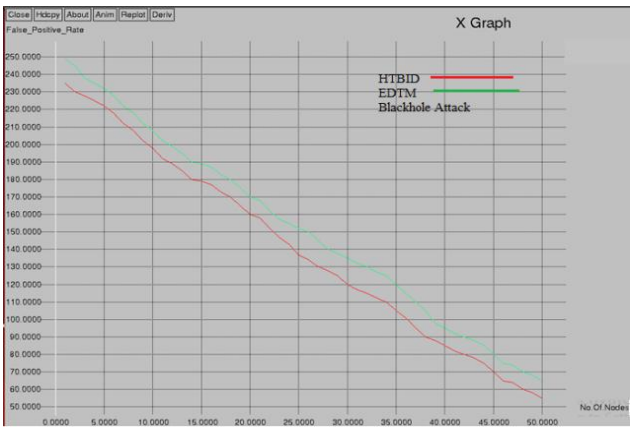

Figure 5. False positive rate for Blackhole attack

Figure 6. shows that Packet delivery ratio (PDR) of HTBID is higher than EDTM in presence of Blackhole attack.

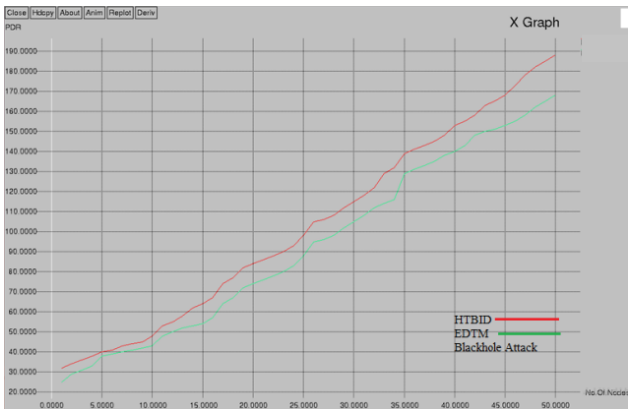

Figure 6. PDR in presence of Blackhole attack

Figure 7. shows that detection rate of HTBID is more than EDTM in presence of Blackhole attack.

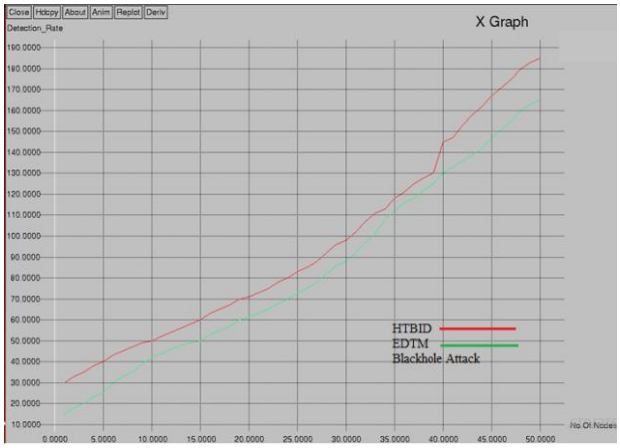

Figure 7. detection rate for Blackhole attack

Figure 8. Shows that false positive rate of HTBID system is less than EDTM model in presence of ONOFF attack.

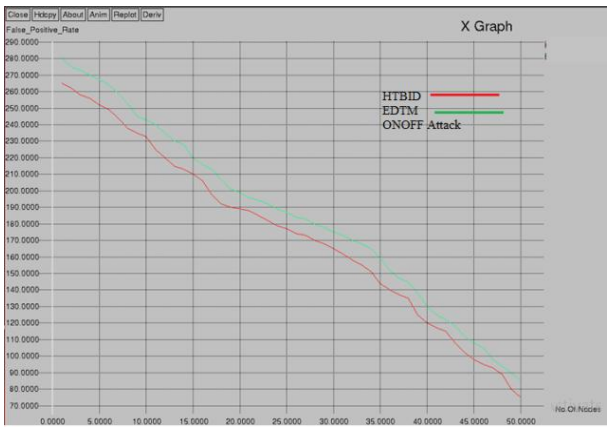

Figure 8. False positive rate in presence of ONOFF attack

Figure 9. shows that Packet delivery ratio (PDR) of HTBID is higher than EDTM in presence of ONOFF attack.

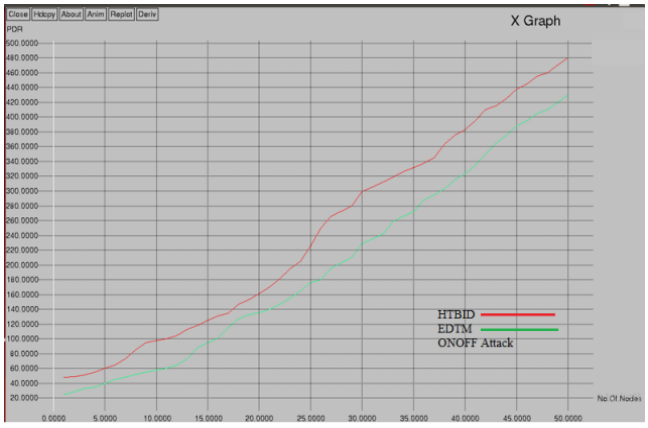

Figure 9. PDR in presence of ONOFF attack

Figure 10. shows that detection rate of HTBID is more than EDTM in presence of ONOFF attack.

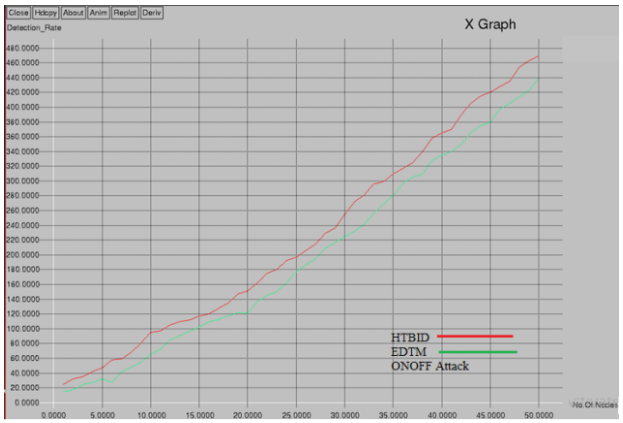

Figure 10. Detection rate in presence of ONFF attack.

CONCLUSION

As nodes in WSN are deployed in open environment, they are more vulnerable to different types of attack. Now days, Trust based Intrusion detection systems have become important to deal with malicious activities in wireless sensor network. In this paper, a Hierarchical Trust based Intrusion Detection [HTBID] system is proposed for cluster based WSN. This system makes use of Hierarchical trust Evaluation protocol [HTEP] for dealing with various attacks WSN. During HTEP, calculation of peer-to-peer trust, CH-to-SN trust and base station-to-CH trust are discussed. This system considers social as well as QoS trust for evaluation of trustworthiness. Results of simulation show that HTBID performs better than EDTM in terms of detection rate, packet delivery ratio while maintaining false positives to lower rate.

REFERENCES

[1] A. R. Dhakne and P. N. Chatur, "Distributed Trust based Intrusion Detection approach in wireless sensor network," 2015 Communication, Control and Intelligent Systems (CCIS), IEEE, Mathura, 2015, pp. 96-101. http://dx.doi.org/10.1109/CCIntelS.2015.7437886

[2] Amol R. Dhakne, Prashant N. Chatur, "TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network," IJCSNS International Journal of Computer Science and Network Security , vol.16, no.12,pp. 1-10, Dec. 2016.

[3] A. R. Dhakne, P. N. Chatur, "Detailed Survey on Attacks in Wireless Sensor Network, Proceedings of the International Conference on Data Engineering and Communication Technology ,"Vol. 469 of the series Advances in Intelligent Systems and Computing , Springer, 2016, pp 319-331. https://dx.doi.org/10.1007/978-981-10-1678-3_31

[4] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 366–379, Oct.–Dec. 2004.

[5] A. R. Dhakne, P. N. Chatur, "Detection of On Off Attack Based On Predectability Trust in Wireless Sensor Network," Proceedings of 64th IRF International Conference, 16th October, 2016, Pune, India. http://iraj.in/up_proc/pdf/245-147849566525-29.pdf

[6] P. B. Velloso, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Trans. Netw. Service Management, vol. 7, no. 3, pp. 172–185, Sep. 2010.

[7] A. da Silva, et al., "Decentralized intrusion detection in wireless sensor networks," in Proc. 2005 ACM Int. Workshop Quality of Service Security Wireless Mobile Netw., pp. 16–23.

[8] M. S. Islam, R. H. Khan, and D. M. Bappy, "A hierarchical intrusion detection system in wireless sensor networks," Computer Science Netw. Security, vol. 10, no. 8, pp. 21–26, Aug. 2010.

[9] C. Budianu, S. Ben-David, and L. Tong, "Estimation of the number of operating sensors in large-scale sensor networks with mobile access," IEEE Trans. Signal Process., vol. 54, no. 5, pp. 1703–1715, May 2006.

[10] R. A. F. Mini, A. A. F. Loureiroa, and B. Nath, "The distinctive design characteristic of a wireless sensor network: the energy map," Computer Commun., vol. 27, no. 10, pp. 935–945, June 2004.

[11] Y. J. Zhao, R. Govindan, and D. Estrin, "Residual energy scan for monitoring sensor networks," in Proc. 2002 IEEE Wireless Commun. Netw. Conf., pp. 356–362.

[12] R. A. Shaikh, et al., "Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[13] Amol R. Dhakne, P. N. Chatur, "A Comprehensive Survey on Intrusion Detection Systems in Wireless Sensor Network," Smart Trends for Information Technology and Computer Communications, Communications in Computer and Information Science (CCIS), Springer Singapore, Vol. 628, pp 541-549, 2016. http://dx.doi.org/10.1007/978-981-10-3433-6_65

[14] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, "Efficient Distributed trust Model in Wireless Sensor Network," IEEE Transactions on Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.

ABOUT THE AUTHORS:

Amol R. Dhakne received B.E. Information Technology in 2010 from Jawaharlal Nehru Engineering College, M.E. Computer Science and Engineering in 2013 from Government College of Engineering both affiliated to Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India. Since from July 2014, he is Ph.D. Research Scholar at Government College of Engineering, Amravati affiliated to Sant Gadge Baba Amravati University, Amravati. His research interests include security, trust management, Intrusion detection, network security, wireless sensor network, mobile ad hoc network.

Dr. P. N. Chatur has received his M.E. degree in Electronics Engineering from Government College of Engineering, Amravati, India and Ph.D. from Amravati University. He has published hundred and ten papers in conferences and journals. His area of research includes Wireless Sensor Network, Artificial Neural Network, Data Mining, Data Stream Mining and Cloud computing. Currently he head of Computer Science and Engineering Department at Government College of Engineering Amravati, Maharashtra, India. At present he is engaged with energy efficiency and security in wireless sensor network.