World Engineering & Applied Sciences Journal 7 (4): 241-249, 2016
ISSN 2079-2204

DOI: 10.5829/idosi.weasj.2016.241.249

Fuzzy Clustering by Local Approximation of Memberships with Decision Tree Based Trust Intrusion Detection System for Clustered Wireless Sensor Networks

[1]S. Nandhakumar and [2]N. Malmurugan

[1]Dhanalakshmi Srinivasan Engineering College, Perambalur, India
[2]Mahendra College of Engineering, Salem, India

Abstract: Security of Wireless Sensor Network (WSN) is always a major thing as it has widespread application in most of the major domains such as battlefield surveillance, healthcare, etc. Basically there are three main components that deal with security of wireless sensor network, prevention, detection and mitigation. But it is very difficult to prevent wireless sensor network always from malicious attacks so it is always important to detect them as early as possible so that the proposed method can react to the attack not harm to wireless sensor network. In this work, a Fuzzy clustering by Local Approximation of Memberships (FLAME) with decision tree based Trust Intrusion Detection System (TIDS) proposed for clustered wireless sensor networks. Initially, it considered the trust which is distributed among some other factors such as energy, reliability and data. It derives and formulates trust such as direct trust and recommendation trust from these factors. Trust based recommendation is integrated with FLAME based verification method to classify normal and abnormal (attacker node and data) of the data sets and node in terms of malicious behaviour. Experimental results show that the proposed FLAME based TIDS achieved better performance compared than existing trust based intrusion detection systems.

Key words: WSN · Trust system · Intrusion detection · Energy · Reliability · FLAME · Decision tree · clustering · Classification · Malicious attack

INTRODUCTION

A Wireless Sensor Network (WSN) normally includes a large number of tiny sensor nodes (SNs) deployed in an operational subject for data sensing, aggregating and processing. WSNs were applied in transportation, agriculture, place of origin security and battlefield functions. The exposure to common environments and the inherent unreliability of wireless transmission make a WSN susceptible to many attacks [1]. SNs deployed in adversarial environments for navy applications also might be compromised through captures and come to be malicious. Moreover, as a result of severe resource constraints of SNs, akin to power, memory and computational power, average energy-ingesting security mechanisms like public key infrastructure [2] and host-headquartered intrusion detection systems [3] may not be possible.

Malicious attacks to WSNs may also be categorized into outsider attacks and insider attacks. Even as most outsider attacks similar to spoofing, replay and Sybil attacks will also be prevented by means of authentication and cryptography, insider attacks are much tougher to deal with. Clearly protection mechanism [4] to WSN encompass three phases comparable to prevention, detection and mitigation depending on whether or not one desires to avoid it from attacks, if one can't preclude it then to discover these attacks and on the end if one is effective with detection then to mitigate (react) it so that it is going to not furnish more harm to community assets or sensor nodes.

Lots of the prevention strategies [5] reminiscent of cryptographic methods, confidentiality, authentication and message integrity have been proposed to restrict security threats in this paper, a Fuzzy clustering by Local Approximation of MEmberships (FLAME) with decision

Corresponding Author: S. Nandhakumar, Dhanalakshmi Srinivasan Engineering College, Perambalur, India.

tree based Trust Intrusion Detection process (TIDS) proposed for clustered WSN to identify Denial of carrier attack, Replay attack, Worm hole attack etc. However these protection solutions fail to make networking environment free from different a couple of attacks acknowledged above. Ordinary safety options can many times care for external attacks but they fail to avert method from inner attacks caused with the aid of taking pictures of sensor node. At any time when prevention approaches fail to preclude attack, the following line of defence is Intrusion Detection system [6]. IDS can become aware of the attack however it cannot avert it. After detection of attack it might probably generate some signal to indicate the detection of attack. Most of the attacks in wireless sensor community aren't going to be avoided so IDS plays principal and colossal role so far as safety of wireless sensor community is concerned. Until now quite a lot of intrusion detection programs have been proposed corresponding to signature established IDS, anomaly established IDS and Specification situated IDS. Most of the IDS face the problems to detect large range of the assaults in wireless sensor community. There are specific restrictions as sensor nodes are restricted through energy, memory and computational power that must be regarded whenever one wants to set up any IDS on sensor nodes.

Mainly the intrusion detection challenge is viewed as a two-class classification difficulty. The intention is to classify patterns of the method behaviour in two categories (normal and abnormal), using patterns of known attacks, which belong to the irregular classification and patterns of the traditional behaviour. The regular and the irregular behaviours in networked computers are tough to predict because the boundaries cannot be well described. This prediction procedure could generate false alarms in lots of intrusion detection methods. Nevertheless, with fuzzy logic, the false alarm rate in picking out intrusive activities can be lowered [7]. Decision trees [8, 9] are the normally used architectures of machine learning and classification programs. They come with a complete record of different training and pruning schemes, a range of discretization (quantization) algorithms and a series of unique learning refinements [8, 9]. The objective of this study is to gain knowledge and modify a new class of decision tree a semi supervised process to improve strong IDS.

In this work, a FLAME clustering with decision tree based TIDS is proposed for clustered wireless sensor network. The trust intrusion detection method will remember trust which is dispensed amongst every other factor such as energy, reliability and data. It derives and formulates trust reminiscent of direct trust and recommendation trust from these reasons. Trust situated recommendation is integrated with FLAME based verification process to classify the data sets and node in phrases of malicious behaviour. Experimental results show that the proposed FLAME established TIDS attained higher performance compared than existing trust based intrusion detection systems. The rest of the paper is prepared as follows: the part 2 discusses related works on trust based intrusion detection systems. Part 3 describes the proposed methodology. Part 4 experiences simulation outcome of proposed procedure. Part 5 concludes the work.

Related Work: Gheorghe *et al*., [10] proposed Adaptive trust administration Protocol, a protocol that adjusts trust and reputation based on node conduct. The protocol involves three phases: the exchanging section, where in expertise is computed founded on these alerts got from TinyAFD, the replacing section, wherein experience associations are exchanged between neighbor nodes then Updating section, where trust and reputation are updated based on knowledge. ATMP has been carried out on prime of TinyOS and has been verified making use of TOSSIM in various attacks to evaluate the evolution of experience, trust and reputation.

Bao *et al*., [11] proposed a trust-based intrusion detection scheme making use of a tremendously scalable hierarchical believe management protocol for clustered wireless sensor networks. It believed a trust metric due to the fact that each Quality of Service (QoS) trusts and social trust for detecting malicious nodes. With arithmetically analyzing peer-to-peer trust evaluation outcome collected from sensor nodes, each cluster head applies trust-established intrusion detection to consider the reliability and maliciousness of sensor nodes in its cluster. Cluster heads themselves are evaluated through the base station. Develops an analytical mannequin based on stochastic Petri nets for performance analysis of the proposed trust-headquartered intrusion detection scheme, as good as a statistical procedure for calculating the false alarm likelihood. It analyzes the sensitivity of false alarms with admire to the minimal trust threshold beneath which a node is regarded as malicious.

Sajjad *et al*., [12] provided neighbor node trust supported intrusion detection process for WSN. In this system, every node observes the trust degree of its neighboring nodes. Based on these trust values, neighboring nodes could also be declared as trustworthy,

risky or malicious. Trustworthy nodes are advocated to the presumptuous engine for packet forwarding reasons. The proposed scheme efficaciously detects hello flood attack, jamming attack and selective forwarding attack by examining the network statistics and malicious node behaviour.

Bao *et al*., [13] proposed an extremely scalable cluster-established hierarchical trust management protocol for WSNs to conveniently deal with selfish or malicious nodes. Here, take into account multidimensional believe attributes derived from communication and social networks to evaluate the total trust of a sensor node. By way of a novel likelihood model describe a heterogeneous WSN comprising a significant number of sensor nodes with vastly unique social and QoS behaviours with the target to give way ground truth node status. In this serves, as a basis for validating this protocol design by evaluating subjective trust generated as a consequence of protocol execution at runtime in opposition to purpose trust got from precise node repute. To demonstrate the utility of this hierarchical trust management protocol, here apply it to believe-based geographic routing and believe-headquartered intrusion detection. For each and every application, identify the pleasant trust composition and formation to maximize utility efficiency.

Mohan Kumar and Ramprasad [14] considered trust based nodes routing for transmission of message from the source to destination. It uses a centralized wireless sensor networks, such that a single head is accountable for gathering all knowledge of sub headers and if intrusion evolves in the community, it overcome through transmitting the information through these trustable nodes. The intruders within the route are discovered via utilising an Intrusion Detection Procedure Protocol (IDSP) thereby through disposing of squalor of communication.

Francesco Buccafurri *et al* [15] proposed the trust-established methods constitute to make sure safety of distributed methods. On this work, a trust-based method was once discussed to make WSNs tolerant towards attacks focusing on their routing layer. It was once shown that how such attacks are tolerated with low overhead in evaluation to unprotected methods.

Mostaque Md and Morshedur Hassan [16] awarded just a few research papers concerning the foundations of intrusion detection systems, the methodologies and excellent fuzzy classifiers utilizing genetic algorithm that are the point of interest of current progress efforts and the solution of the obstacle of Intrusion Detection approach to offer an actual world view of intrusion detection.

Nabil *et al*. [17] offered a survey on current Intrusion Detection systems and some open research issues involving WSN protection. Anomaly-based IDSs are light-weight in nature; nonetheless they devise extra false alarms. Signature-founded IDSs are compatible for moderately giant-sized WSNs; however they've some overheads comparable to updating and inserting new signatures. Cross layer IDSs are as a rule no longer recommended for networks having resources obstacles, as more energy and computation are required for replacing multilayer parameters.

Wenchao Li *et al* [18] proposed a new intrusion detection system situated on k-nearest neighbor classification algorithm in WSN. This procedure separated abnormal nodes from normal nodes through looking at their irregular behaviors and analyse parameter resolution and error expense of the intrusion detection process. This approach has accomplished effective, speedy intrusion detection via improving the wireless ad hoc on-demand distance vector routing protocol.

Chia-Fen Hsieh *et al*. [19] proposed a lightweight Ontology-Headquartered Wireless Intrusion Detection System (OWIDS). It utilized ontology to a Patrol Intrusion Detection Method (PIDS). A PIDS is used to realize anomalies via detection knowledge. The method constructs the connection of the sensor nodes in ontology to increase PIDS robustness. The sensor nodes preload evaluation ways without detection capabilities. The procedure transfers a portion of the detection information to become aware of anomalies. The memory requirement of a PIDS is decrease than that of other ways which preload whole IDS.

Proposed Methodology: In this section, the FLAME with decision tree based TIDS is discussed in given below sections. The trust value calculation and malicious node detection also explained.

System Overview: Fig 1 shows that the overall process of proposed system. It shows the a Fuzzy clustering by Local Approximation of MEmberships (FLAME) with decision tree based Trust Intrusion Detection System (TIDS) for clustered wireless sensor networks. It considered the trust based on energy, reliability and data. It derives and formulates trust such as direct trust and recommendation trust from these factors. Trust based recommendation is integrated with FLAME based verification method to classify the data sets and node in terms of malicious behaviour [20].

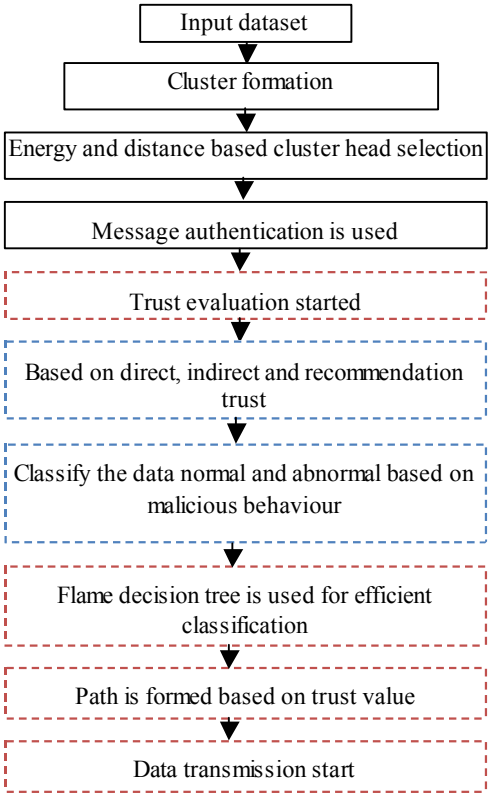

Fig. 1: overall process of proposed system

Input Data Set: The KDD Cup 1999 Intrusion detection contest data [20] (KDD cup 99 Intrusion detection data set) is used in this experiments. This data was prepared by the 1998 DARPA Intrusion Detection Evaluation program by MIT Lincoln Laboratory. Lincoln labs acquired nine weeks of raw TCP dump data. The raw data was processed into connection records, which consist of about 5 million connection records. The data set contains 24 attack types. These attacks fall into four main categories: DOS, Probe, u2r and r2l. The data set has 41 attributes for each connection record plus one class label. The data set for proposed experiments contained 37016 records which were randomly generated from the MIT data set. Random generation of data include the number of data from each class proportional to its size. This data set is again divided into training data with 29612 records and testing data with 7404 records. The data is partitioned into the two classes of ‘‘Normal’’ and ‘‘Attack’’ patterns where Attack is the collection of four classes (Probe, DOS, U2R and R2L) of attacks. The objective is to separate normal and attack pattern to make classifier into two class classifier. Only the 34 numeric features are used in this experiment.

Cluster Formation and Message Authentication: The cluster is created on the foundation of the weight project for all nodes within the network. Weight challenge is done to assess the precedence sensor nodes. The priority raises with the weight of a sensor node. Cluster units are determined in step with this precedence. The base station computes the weight for each sensor node taking two explanations under consideration. The distance between the node and base station is regarded as one of the crucial enormous motives for cluster formation. The node energy can be notion of as another essential element for cluster formation.

Distance: The distance between node and base station are measures using given formula

$$d\ (N,b)\ =\ \sqrt{\sum_{i=1}^{n}(N_i - b_i)^2} \tag{1}$$

where b=base station, N-node.

Energy: The total energy E_t consumed

$$E_t(s_i\ ,d) = \begin{cases} s_i E + s_i \varepsilon_{fs} d^2, d \le d_0 \\ s_i E + s_i \varepsilon_{mp} d^2, d > d_0 \end{cases} \tag{2}$$

$$d_o = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \tag{3}$$

where E represents the energy consumed to transmit or receive 1 bit message; ε_{fs} is the free-space signal amplification coefficient and ε_{mp} is the multi-path fading signal amplification coefficient and their value depend on the circuit amplifier model and *d* represents the distance between transmitter and receiver; s_i is the bit amount of sending information.

The message receiver will have to be able of verifying whether or not an obtained message is sent by means of the node that is official or by a node in a precise group. In any other case stated, the enemies cannot act to be a harmless node and introduce faux messages into the network community without being seen. The authentication is supplied based on Rivest-Shamir-Adleman (RSA) encryption and decryption algorithm.

Trust Value Calculation: The proposed system considers direct trust and recommendation trust to evaluate the trustworthiness of sensor node in FLAME based TIDS model.

Direct Trust: The direct trust received based on message exchange behaviour, energy trust and data trust. Sensor nodes in WSN constantly are in contact with each and every different to perform specified networking challenge. However at the same time message exchange can be unsuccessful because of nature of wireless network causing loss of packets. Unsuccessful communiqué may also be induced by way of malicious nodes or unstable communication channel. Consequently simply evaluating the communiqué trust to get direct trust is not adequate. Aside from that as any communication consumes designated quantity of power, calculate the energy trust, if communiqué with object nodes requires the extra energy than the energy wanted for verbal exchange then conclude that object node is malicious node. Energy trust is used to verify whether or not node is equipped to participate in intended perform or not. Data trust is evaluated to determine whether object node is able to send the packets that are needed by subject node. If object node alterations the packets and does unique modification in data then it is viewed as malicious one. So the direct believe $T_{c\&d}$ is calculated based on three factors such as Communication trust t_c, energy trust t_e and data trust t_d as follows:

$$T_{ced} = w_c t_c + w_e t_e + w_d t_d \quad (4)$$

where $w_c + w_e + w_d = 1$. w_c, w_e, w_d are the weights related to communiqué trust, power trust and knowledge trust respectively and these weights are not negative. The weight values are weight varies from 0 to l relying on whether or not subject node and object node are one hop neighbour or multi-hop neighbour. If two nodes are equipped to straight establish trust then weight price $w_d = 1$ and recommendation trust and indirect trust will not be considered as $w_r = w_i = 0$; sometimes even though two nodes are one hop neighbour subject node can take recommendation of object node from other node at that time weight values are distributed among WD and WR. If two nodes are not able communicate directly then whole weight is given to indirect trust.

Communication trust (t_c) of sensor node is calculated based on successful (s) and unsuccessful (u) interactions among sensor nodes over some time period (O, t)

$$t_c = \frac{s}{s+u} \quad (5)$$

Energy trust refers back to the perception of one node that different node still has sufficient energy to perform its meant operate. Malicious nodes continuously consume further quantity of energy to launch malicious attack. Energy prediction items can be utilized to foretell energy of sensor node. Energy consumptions value of sensor node maintains stable value if atmosphere stipulations do not exchange ordinarily. Energy trust (T_e) is calculated based on energy consumption rate E_t that ranges from 0 to 1. For calculating consumption rate we calculate the residual energy E_{res} First define energy threshold E_{th} whenever residual energy is falls below threshold conclude that sensor node is not competent to perform intended function and consider energy trust t_e as 0. Otherwise calculate energy consumption rate E_c based on ray projection method [21].

$$t_e = \begin{cases} 0, if\ E_{res} < E_{th} \\ 1 - E_c, else \end{cases} \quad (6)$$

The trust component knowledge is used to calculate trustworthiness with admire to information in the community. Attacks such as the stealthy attack can result on the information aggregation. Sensed knowledge expertise can be used to calculate knowledge trust. Trust value of information is defined as

$$t_d = l - 2\int_m^x f(x)dx \quad (7)$$

Recommendation Trust: Most of the instances at any time when direct communication conduct is just not feasible between subject node and object node, then the recommendations are taken from recommender for trust calculation. However again it's not certain whether the recommendations that subject node will get are correct or now not. So there may be must evaluation the advice believe to come to a decision whether ideas that field node is getting are authentic or not. Recommendation trusts is calculated based on major factor such as reliability of recommender. Outlier detection schemes can be used to judge whether or not certain recommender is Recommendation or not. Reliability of Recommender T_r is calculated as follows:

$$T_r = 1 - |T_r^c - T_{avg}^c| \quad (8)$$

where T_r^c the recommendation value of object node c is reported by recommender r^i and T_{avg}^c is average of all recommendations.

Flame Decision Tree Based Classification: In this proposed system, the node with the absolute best value of the criterion is chosen and dealt with it as a candidate for additional refinement. The process is repeated through choosing probably the mainly varied node out of all final nodes. Then the growth of the tree is applied via increasing the nodes and building their consecutive levels that seize extra details of the arrangement. It's noticeable that the node expansion leads to develop in either the depth or width (breadth) of the tree. The pattern of the development could be very much implied with the aid of the traits of the information as good as influenced with the aid of the quantity of the clusters. As soon as the tree has been developed, this approach used the decision tree concept to classify an unknown pattern or predict the corresponding output of the pattern. It traverse the tree by using commencing from the basis node and then identifying a direction in line with the similarity calculations to move down from the present degree to the subsequent level except a leaf node is reached. In the end, the nearby linear model of the attained leaf node is calculate the output of the unknown pattern.

FLAME clustering is a core sensible a part of the overall tree. It builds the clusters and supplies its full description. Standard FLAME is an omnipresent method of information granulation. The FLAME algorithm is an example of an object-oriented fuzzy clustering wherever the clusters are designed by means that of a reduction of some goal perform.

Flame Clustering: Fuzzy clustering by using Local Approximation of MEmberships (FLAME) [22] defines clusters within the opaque divisions of a dataset and performs cluster assignment based on the nearby relationships among nodes. The FLAME constructs K-Nearest Neighbors graph used for recognize the cluster centers and outliers. Proteins with the very best regional density referred to as Cluster supporting Objects (CSO) and proteins with a local density scale down than a threshold are referred to as outliers. CSOs are allocated through full membership to stand for it as cluster centers. Outliers are allocated with full membership to the outlier group. After that the fuzzy memberships are allocated to remaining proteins by means of altering degrees of memberships to the cluster helping objects. There's no need to specify the predefined number of clusters. It usually determines the numbers of cluster and outliers. It needs the number of K-Nearest Neighbors and trust threshold worth for outliers as preliminary parameters. A simple output node representation (centroids) is regarded, to use the choice tree within the classification mode.

Pseudo Code for Flame Decision Tree

Step 1: the structure information is extracted from the dataset

- a neighborhood graph is constructed to connect each node to its K-Nearest Neighbors (KNN)
- a density for each node is estimated based on its proximities to its KNN
- Nodes are classified into 3 types
  - Cluster Supporting Object (CSO): node with density higher than all its neighbors
  - Cluster Outliers: node with density lower than a predefined threshold and lower than all its neighbors
  - The rest of the nodes

Step 2: Local/Neighbourhood approximation of fuzzy memberships

- Initialization of fuzzy membership
  - With fixed and full membership is assigned for each CSO to itself to signify one cluster
  - Every outliers are assigned with fixed and full membership to the outlier group
  - Then the rest are allocated with equal memberships to all clusters and the outlier group
- Then all type 3 objects fuzzy memberships are updated by a converging iterative procedure called Local/Neighborhood Approximation of Fuzzy Memberships, wherein the fuzzy membership of each object is updated by a linear combination of the fuzzy memberships of its nearest neighbors.

- Cluster construction from fuzzy memberships in two possible ways
  - One-to-one node-cluster task, to assign each object to the cluster in which it has the highest membership
  - One-to-many node-cluster task, to assign each object to the cluster in which it has a membership higher than a threshold.

Step 3: Decision tree applied to classify the data

- Normal behaviour of data (node information) in which it has the highest trust value.
- Abnormal behaviour of data (node information) in which it has a trust value higher than a threshold.

The proposed system is observed that the decision tree size and number of leaf nodes comparatively less with division thus reducing the complexity of the tree. The classification accuracy also significantly improved due to the division thus resulting in effective Intrusion Detection System.

RESULTS AND DISCUSSION

In this section, the proposed FLAME based TIDS system performance is evaluated and its performance results are compared to existing methods such as Effective Trust based Intrusion Detection System (ETIDS) and Trust based Intrusion Detection System (TIDS).

Simulation Model and Parameters: The attacks withstand by proposed system are Denial of Service attacks, Replay attack, Worm hole attack etc. In previous work, all these attackers are not solved perfectly. Because of analytical model was not proved for attackers. The proposed FLAME based TID is simulated with Network Simulator tool (NS 2.34). In proposed simulation, 100 sensor nodes move in a 1200 meter x 1200 meter square region for 100 seconds simulation time. Here, assume each node moves independently with the same average speed. All nodes have the same transmission range of 200 meters. The simulated traffic is Constant Bit Rate (CBR). The proposed system simulation settings and parameters are summarized in Table 1.

Performance Evaluation: The performance of proposed system is evaluated based on the following metrics.

Energy Consumption: The average energy consumed by each node during the given simulation time and it expressed in Joules (J).

Fig 2 shows that the graphical representation of energy consumption for different number of nodes in WSN. The FLAME with TIDS algorithm has low energy consumption when compared with the existing ETIDS, TIDS. The energy for each and every node is calculated and cluster formation is done based on the energy values.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Fig 3 shows the results of Mobility Vs end to end delay. From the results, the proposed FLAME with TIDS has less delay than existing ETIDS, TIDS. End to end delay should kept minimum in order to satisfy QoS.

Table 1: simulation parameters

No. of Nodes	100
Area Size	1200 X 1200
Mac	802.15.4
Radio Range	200m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	512 bytes
Protocol	LEACH

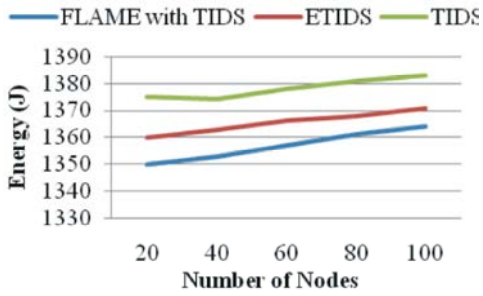

Fig. 2: Comparison of Energy consumption vs. Number of Nodes

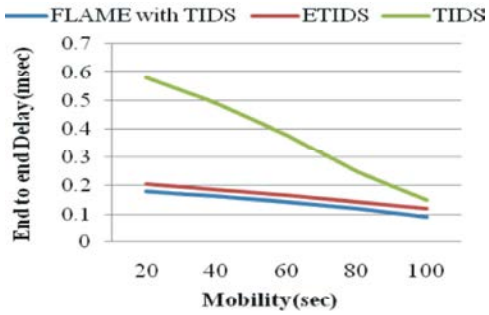

Fig. 3: Mobility Vs End to end delay

The proposed system reduces delay by means of cluster based routing. Network partitioning will be reduced by integrating this routing in all networks.

Communication Overhead: Communication overhead can be defined as the average number of control and data bits transmitted per data bits delivered. Control bits include the cost of location updates in the preparation step and destination searches and retransmission during the routing process.

Fig 4 shows the results of Pause time Vs Communication overhead. From the results, the proposed FLAME with TIDS achieved less overhead than previous ETIDS, TIDS. It is because of link stability determination. Cluster head chooses only high stable link for data forwarding. So the network delivery rate is getting increased. Packet overhead will be suppressed because of link quality and reliability of neighbor nodes.

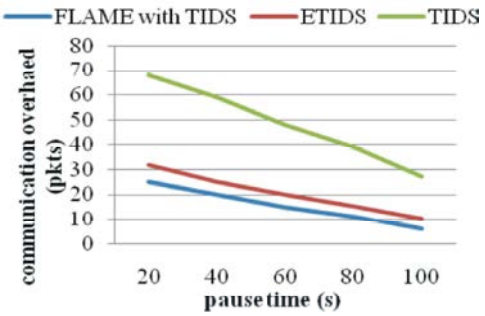

Fig. 4: Pause time Vs Communication Overhead

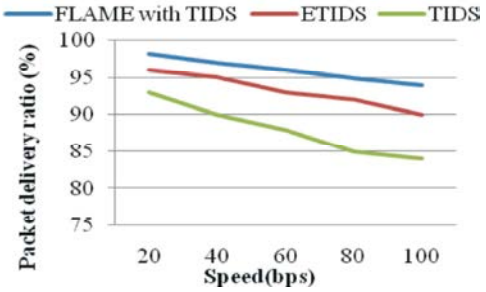

Fig. 5: Speed Vs Packet Delivery Ratio

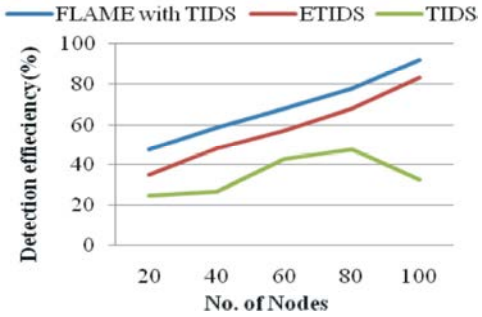

Fig. 7: Speed Vs Packet Integrity Rate

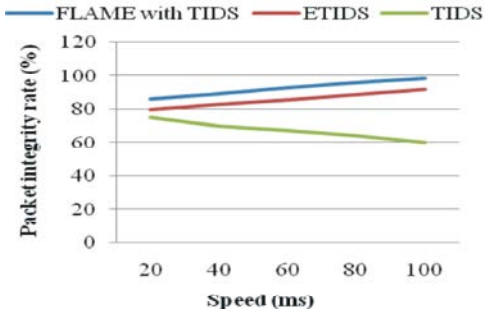

Fig. 6: No. of Nodes Vs Detection Efficiency

Packet Delivery Ratio: The delivery rate is defined as the ratio of numbers of messages received by the destination and sent by senders. The best routing methods employing this metric are those that guarantee delivery in which message delivery is guaranteed assuming "reasonably" accurate destination and neighbour location and no message collisions.

Fig 5 shows the results of packet delivery ratio for the speed. From the results, the proposed FLAME with TIDS achieved more packet delivery ratio than previous ETIDS, TIDS. The proposed system comprises two major aspects i.e. malicious detection and network authentication. Packet is delivered via reliable nodes through stable link. Successfully all the packets are delivered to the destination.

Malicious Node Detection Efficiency: Fig 6 shows the results of detection efficiency for the nodes 10, 20, 30….100 scenarios. The proposed FLAME with TIDS achieved more detection rate than the previous ETIDS, TIDS. Because of cluster based routing. In this routing, link stability is maintained and malicious nodes are identified using the trust recommendation. Therefore the vulnerability of malicious nodes is reduced.

Network Packet Integrity Rate: Fig 7 shows the results of Speed Vs Packet Integrity Rate. From the results, the proposed FLAME with TIDS has high integrity than previous ETIDS, TIDS. The proposed system increases network packets integrity based on encryption and decryption scheme performance.

CONCLUSION

Trust models have become very important as far as detection of malicious behaviour is concerned. The proposed FLAME with decision tree based TIDS model not only considers communication behaviour to detect trustworthiness of sensor node but also considers some other factors of trust which are distributed in energy, data trust, reliability, communication trust etc. Initially, the calculation of trust is has been discussed. It based on three trusts such as direct trust and recommendation trust. Secondly, FLAME decision tree with trust used to classify patterns of the system behaviour in to normal and abnormal of two categories, using patterns of known attacks is fit in to the abnormal class and patterns of the normal behaviour is normal. The experimental result shows that the FLAME with TIDS has achieved high packet delivery ratio, detection efficiency, packet integrate rate and less energy consumption, delay and

communication overhead compared than existing schemes. In future, the classification is focused with any other machine learning algorithms and trust calculation is focused with any other parameters.

REFERENCES

1. Chen, X., K. Makki, K. Yen and N. Pissinou, 2009. Sensor network security: a survey, IEEE Communication Surveys & Tutorials, 11(2): 252-73.
2. Mishra, A., K. Nadkarni and A. Patcha, 2004. Intrusion detection in wireless ad hoc networks, IEEE Wireless Communications, 11(1): 48-60.
3. Zhang Y., W. Liu, W. Lou, Y. Fang and Y. Kwon, 2005. AC-PKI: anonymous and certificate less public-key infrastructure for mobile ad hoc networks, 40th IEEE International Conference on Communications, pp: 3515-3519.
4. Butun, I., S.D. Morgera and R. Shankar, 2014. A Survey of Intrusion Detection Systems in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, 16(1).
5. Singh, S.K., M.P. Singh and O.K. Singh, 2011. A Survey on Network Security and Attack Defence Mechanism for Wireless Sensor Network, International Journal of Computer Trends and Technology.
6. Abduvaliyev, A, A.K. Pathan,., J. Zhou, R. Roman and W.C. Wong, 2013. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, 15(3).
7. Gomez, J. and D. Dasgupta, 2001. Evolving fuzzy classifiers for intrusion detection, Proceedings of the 2002 IEEE Workshop on the Information Assurance, West Point, NY, USA.
8. Quinlann, J.R., 1986. Induction of decision trees, 1: 81-106.
9. Alexander, W.P. and S. Grimshaw, 1996. Tree regression, J. Computational Graphical Statistics, 5: 156-175.
10. Gheorghe, L., R. Rughinis and R. Tataroiu, 2013. Adaptive trust management protocol based on intrusion detection for wireless sensor networks. In Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition IEEE, pp: 1-7.
11. Bao, F., I.R. Chen, M. Chang and J.H Cho, 2011. Trust-based intrusion detection in wireless sensor networks. In Communications (ICC), 2011 IEEE International Conference on IEEE, pp: 1-6.
12. Sajjad, S.M., S.H. Bouk and M. Yousaf, 2015. Neighbour Node Trust based Intrusion Detection System for WSN. Procedia Computer Science, 63: 183-188.
13. Bao, F., I.R. Chen, M.Chang and J.H. Cho, 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, Network and Service Management, IEEE Transactions on, 9(2): 169-183.
14. Kumar Mohan and V.Ramprasad, 2014.Trust Management Based Intrusion Detection in Wireless Sensor Networks, International Journal of Innovative Research in Science, Engineering and Technology, pp: 1025-1028.
15. Francesco Buccafurri, Luigi Coppolino, Salvatore D'Antonio, Alessia Garofalo, Gianluca Lax, Antonino Nocera and Luigi Romano, 2014. Trust-Based Intrusion Tolerant Routing in Wireless Sensor Networks, Springer, 8666: 214-229.
16. Mostaque Md and Morshedur Hassan, 2013.Current Trends on Intrusion Detection System, Genetic algorithm and Fuzzy Logic, International Journal of Distributed and Parallel Systems, 4(2): 35-47.
17. Nabil Ali Alrajeh, S. Khan and Bilal Shams, 2013. Intrusion Detection Systems in Wireless Sensor Networks: A Review, International Journal of Distributed Sensor Networks, 3: 1-7.
18. Wenchao Li, Ping Yi, Yue Wu, Li Pan and Jianhua Li, 2014. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network, Journal of Electrical and Computer Engineering, Hindawi Publication, 1-9.
19. Hsieh Chia-Fen, Rung-Ching Chen and Yung-Fa Huang, 2014. Applying Ontology to a Patrol Intrusion Detection System for Wireless Sensor Networks, International Journal of Distributed Sensor Networks, Hindawi Publication, pp: 1-15.
20. Lim, H.S., Y.S. Moon and E. Bertino, 2010. Provenance based Trustworthiness Assessment in Sensor Networks, in Proc. 7th In!. Workshop Data Manage. Sens. Netw, pp: 2-7.
21. Limin Fu and Enzo Medico, 2007. FLAME, a novel fuzzy clustering method for the analysis of DNA microarray data, BMC Bioinformatics, 8: 3.
22. Cheng Pu, Minghua Zhu and aXianzhong Liu, 2014. Distributed T-Distribution-Based Intrusion Detection in Wireless Sensor Networks, Springer, 295: 313-323.