Research Journal of Applied Sciences, Engineering and Technology 9(9): 760-769, 2015
DOI:10.19026/rjaset.9.2622
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: October 05, 2014 Accepted: November 26, 2014 Published: March 25, 2015

Research Article

Fuzzy Based Anomaly Intrusion Detection System for Clustered WSN

[1]Sumathy Murugan and [2]M. Sundara Rajan
[1]Research and Development Centre,
[2]Bharathiar University, Coimbatore-641046, India

Abstract: In Wireless Sensor Networks (WSN), the intrusion detection technique may result in increased computational cost, packet loss, performance degradation and so on. In order to overcome these issues, in this study, we propose a fuzzy based anomaly intrusion detection system for clustered WSN. Initially the cluster heads are selected based on the parameters such as link quality, residual energy and coverage. Then the anomaly intrusion is detected using fuzzy logic technique. This technique considers the parameters such as honest, energy level, unselfishness and prediction variance of each cluster member and provides the optimal trust threshold of the node as the result. By simulation result, we show that the proposed technique enhances the detection accuracy and reduces the false positive rate.

Keywords: Anomaly IDS, cluster, fuzzy logic, metrics, WSN

INTRODUCTION

Wireless Sensor Networks (WSN): Wireless Sensor Networks (WSN) generally composed of a collection of self-organizing, low-power, low-cost, autonomous tiny devices called wireless sensor nodes spatially distributed by sensors to monitor and affect the environmental conditions like temperature, sound, vibration, pressure, motion or pollutants, at different locations. The sensor nodes self-organize collaborate with each other to estimate various phenomena varying in time and space and transmit the sensed data to a central node called base station for further processing and analysis. The neighboring sensor nodes sense highly correlated data with the same unknown distribution. The nodal architecture is different for applications and designed for data collection, data management, data transfer and power supply. It has a wide area of applications like potential applications including burglar alarms, medical monitoring and emergency response, monitoring remote, target tracking in battlefields, disaster relief networks, military, early fire detection in forests and environmental monitoring (Zhang, 2009; Tiwari *et al*., 2009; Livani and Abadi, 2010, 2011; Hsieh *et al*., 2011; Coppolino *et al*., 2013; Bhuse and Gupta, 2006).

The broadcasting nature of transmission medium and the limited power supply, bandwidth, memory and computational capabilities of sensor nodes pay the way for many security attacks and faults in WSNs. In addition, the nodes are often placed in a hostile or dangerous or unreachable environment without physical protection (Zhang, 2009; Livani and Abadi, 2010, 2011; Hsieh *et al*., 2011; Coppolino *et al*., 2013; Li, 2010).

Anomaly intrusion detection system in WSN: An attacker can easily capture a WSN node physically, alter its code and get private information like cryptographic key i.e., the intruders can easily compromise sensor nodes and use them to transmit malicious information targeting base station or server. These nodes try to overwhelm the network with unnecessary updates, data and other traffic for depleting the limited resources like bandwidth, power, etc., (Reznik *et al*., 2009; Rassam *et al*., 2013). The critical nature of WSN applications rise various attacks like sinkhole, selective forwarding, wormhole, blackhole and hello flooding attacks on them, either for financial gain or for malicious and illegal purposes (Livani and Abadi, 2011; Abduvaliyev *et al*., 2013; Jurdak *et al*., 2011). Wormhole attack which has no effective prevention method and masquerade attacks are dangerous since they hide and present them as legitimate nodes though adversaries can run other attacks. In these cases, once the nodes become compromised, protecting the information by encryption, key management, authentication, privacy, security routing protocols, high-level security services cannot work out but it needs an intrusion detection system to detect malicious events in the system and to prevent the intruder from causing damages to the network. An Intrusion Detection System (IDS) can acquire attack technique information to assist in the development and execution of preventive techniques. Hence an anomaly

Corresponding Author: Sumathy Murugan, Research and Development Centre, Bharathiar University, Coimbatore-641046, India

detection scheme is required to deployed in each individual sensor node based on WSN characteristics to detect anomalous data with acceptable accuracy while minimizing communication overhead and to clean them (Reznik *et al*., 2009; Xiao *et al*., 2009; Livani and Abadi, 2010; Bhuse and Gupta, 2006; Li, 2010).

Some existing intrusion detection methods like rule based and misuse detection cannot be applied to WSN due to WSN characteristics like limited power, bandwidth constraint, limited computation capabilities of nodes and the large number of nodes, widely distribution of nodes, open communication medium, network dynamics and enormous sensed data stream (Xiao *et al*., 2009).

The limited resources of WSN impose challenges in an intrusion detection design. The intrusion detection differentiates the normal system behavior from the behavior of a system under attack. But many WSN configurations could not differentiate them. A detection log file is hard to create due to limited memory and hardware resources. As the sensor nodes are non recoverable and disposed after the application, a log file is hard to recover due to the possible dangerous environment. Frequent sensor node failure is another issue in IDS design (Reznik *et al*., 2009; Jurdak *et al*., 2011).

Problem summary: The existing works on intrusion detection face lot of complexities like increased computational cost as in Livani and Abadi (2010) and Usman *et al*. (2012) much time consumption as in Hsieh *et al*. (2011), increased false positives as in Sedjelmaci *et al*. (2012), increased packet loss rate and decreased detection rate (Sun *et al*., 2013), performance degradation (Riecker *et al*., 2012), ignoring monitoring techniques in control process (Pugliese and Santucci, 2013) and ignoring constraints like detection time, window size, false alarm rate etc., (Stelte and Rodosek, 2013), predicatability and information redundancy occurrence (Xie *et al*., 2015).

Objectives: To overcome the above issues, we should develop an anomaly based intrusion detection system to better detect anomalies in the network efficiently with high detection rate, higher performance, low false positives, low cost and less time consuming. The anomalies in the system should be removed from the network. Also our IDS should detect the false positives efficiently and should consider metrics like detection time, window size, false alarm rate etc.

Also the intrusion detection system may utilize other metrics like similarity to measure the difference between two data segments if without spatial correlations.

Problem definition: To overcome the above issues, we propose to develop a hierarchical trust management protocol by estimating trust component considering metrics like intimacy, honesty, energy and unselfishness (Bao *et al*., 2012). This protocol maintains trust at two levels: SN-level trust evaluating sensor nodes of same cluster by each sensor node and CH-level trust evaluated by each cluster head of other cluster heads and sensor nodes in its clusters. Then we develop a trust-based IDS algorithm utilizing the protocol which relies on choosing a system minimum trust threshold below which a node is considered compromised and should be excluded from sensor reading and routing duties. The false positives and false negatives in IDS are reduced by choosing minimum threshold. It can also be minimized by using an optimal trust threshold.

However individual sensor readings are subjected to noise. These noises and errors in estimation were not considered in this scheme.

In this study, we propose to develop anomaly IDS for clustered WSN using Fuzzy logic technique.

LITERATURE REVIEW

Livani and Abadi (2010) have proposed a distributed energy-efficient approach to detect anomalies in sensed data in a WSN which was caused by compromised or malfunctioning nodes. A Distributed Principal Component Analysis (DPCA) and Fixed-Width Clustering (FWC) were employed to establish a global normal profile and for anomaly detection. Weighted coefficients and a forgetting curve were deployed for the established normal profile's periodical updating. The scheme achieved high accuracy and reduced communication overhead in the network and energy consumption. However there was an increased computational cost.

Hsieh *et al*. (2011) has proposed lightweight ontology-based IDS to reduce energy consumption and the isolation tables avoid detecting anomaly repeatedly. Ontology was deployed to construct relationship between sensor nodes to detect Sybil attack without cryptograph method. However it is time consuming.

Bao *et al*. (2012) have proposed a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks for dealing with selfish or malicious nodes effectively. The overall trust of a sensor node was evaluated by considering multidimensional trust attributes from communication and social network. The hierarchical trust management protocol was applied to trust-based geographic routing and trust-based intrusion detection.

Sedjelmaci *et al*. (2012) have proposed an intrusion detection framework for a Cluster-based WSN (CWSN) utilizing the advantage of anomaly and signature detection like high detection rate and low false positive respectively. However there was an increased false positives.

Usman *et al*. (2012) proposed a mobile agent based anomaly detection mechanism for WSHSNs utilizing devices' heterogeneous nature in smart home to detect anomalies effectively. The anomaly detection infrastructure was installed at resource rich nodes such as Cluster Heads (CHs). The proposed scheme was

efficient in utilization of memory, reducing network load and reduction in overall computational cost of the network. However it consumed much cost.

Sun *et al*. (2013) proposed integration of system monitoring modules and intrusion detection modules in the context of WSNs. Then an Extended Kalman Filter (EKF) based mechanism was proposed for false injected data detection by which future states were predicted utilizing the monitoring behaviors of its neighbors so that to set up a normal range of the neighbors' future transmitted aggregated values. The effective way of utilizing EKF to create an effective local detection mechanism was described. However with increased packet loss rate, detection rate decreases.

Riecker *et al*. (2012) developed three decentralized, lightweight data anomaly detection mechanisms on sensor nodes. These algorithms were described with a real dataset where plausible attacks were added. However these decentralized algorithms do not perform like the algorithms employing supervised learning.

Pugliese and Santucci (2013) proposed a reliable anomaly behavior detection technique in monitoring critical infrastructures through resource constrained devices like WSNs. Here a non-parametric detection technique namely "MV-estimator-based" was proposed where the sample mean and the sample variance computed from observations and behavior classification was performed by defining regions in the MV-estimator space instead of the observations space. However the control process ignored monitoring techniques.

Stelte and Rodosek (2013) proposed an anomaly-based approach Intrusion Detection System (IDS) optimized for ZigBee-based WSN to protect ZigBee-based WSN nodes against KillerBee supported attacks. The Killer Bee attack procedure was described and a ZIgbee transceiver guarding approach was proposed. The anomaly based detection engine thwart attacks on Zigbee transceiver. However the detection time, window size, false alarm rate were not given much importance here.

Xie *et al*. (2015) proposed a new segment-based anomaly detection technique to deal with long-term anomalies by exploiting the spatial correlation existed among neighboring sensed measurements, with its detector realized through a trackable parameterized statistical quantity. Also, the sample covariance matrix was approximated based on Spearman's rank correlation coefficient and differential compression concepts to reduce the computational cost. However, the scheme relied on assuming the data are spatially correlated as this is the only situation in which predictability and information redundancy occur.

MATERIALS AND METHODS

Overview: In this study, we propose a fuzzy based anomaly intrusion detection system for clustered WSN. Initially the cluster heads are selected based on the parameters such as link quality, residual energy and coverage. Then the anomaly intrusion is detected using fuzzy logic technique. This technique considers the parameters such as honest, energy level, unselfishness and prediction variance of each cluster member and provides the optimal trust threshold of the node as the result.

Estimation of metrics: Let N_i and N_j be the neighbor nodes.

Let C_{th} be the pre-defined threshold value of dishonest behavior of node.

Honest (H_{ij}): It is the conviction of N_i that N_j is honest based on N_i's direct observations towards N_j. It is estimated by monitoring the count of suspicious dishonest experience (C) of N_j by N_i at time t.

If count>C_{th}

Then

$$H_{ij} = 0$$

Else

$$H_{ij} = 1 - \frac{C}{C_{th}}$$

End if

H_{ij} = 0 reveals that when the count exceeds the pre-defined threshold, N_j is considered totally dishonest at time t.

Energy (E_{ij}): It is the conviction of N_i that N_j contains sufficient energy to performs intended function. It is estimated as follows.

The total energy spent by the transmitter for transmitting x bits message through distance d is given using Eq. (1):

$$E_{tx} = E_e.x + E_a.x.d^2 \quad (1)$$

where,

E_e = Electronics energy

E_a = Amplifier energy

The total energy consumed by the receiver is given using Eq. (2):

$$E_{rx} = E_e.x \quad (2)$$

The residual energy of each node (E_{res}) following one data communication is estimated using Eq. (3) (Zhao *et al*., 2012):

$$E_{res} = [E_i - (E_{tx} + E_{rx})] \quad (3)$$

where, E_i = initial energy of the node

Unselfishness (U_{ij}): This metric offer the degree of unselfishness of N_j as estimated by N_i based on direct observations over (0, t). N_i gives high priority to recent interaction experiences when compared to old experiences during unselfishness estimation (Bao *et al*., 2012).

Table 1: Format of hello message

Node ID	Sequence number	Residual energy (E_{res})	Link Quality (LQ)	Node coverage (C_n)

Prediction Variance (V): CH separately obtains the prediction variance of each node (Xie *et al*., 2015). The estimation of prediction variance is as follows.

Consider the cluster of sensor nodes (cluster formation is shown in below section).

Let $P = \{Q_1, Q_2, \ldots, Q_n\}$ be the real-valued random values of nodes measured during time t.

where, 1, 2,…., n are total number nodes.

Any variable $Q \in W$ is estimated by linear combination of remaining variables:

$$\hat{P} = P - \{Q\} \tag{4}$$

i.e.,

$$Q = \bar{Q} + \beta = \sum_{i=1, Q_i \in \hat{P}}^{n-1} w_i Q_i + \beta \tag{5}$$

$\bar{Q}$ = Estimator
w = Weight
β = Estimation error

The prediction variance is estimated using the following Eq. (6):

$$\begin{aligned} V(\alpha) &= Z - W^Y (1.\vartheta + M) \\ &= Z - \begin{bmatrix} M \\ 1 \end{bmatrix}^Y \begin{bmatrix} R \\ \vartheta \end{bmatrix} \\ &= Z - \begin{bmatrix} M \\ 1 \end{bmatrix}^Y \begin{bmatrix} O & 1 \\ 1^Y & 0 \end{bmatrix}^{-1} \begin{bmatrix} M \\ 1 \end{bmatrix} \end{aligned} \tag{6}$$

Z = Same covariance between two variables
M = Sub-vector

The prediction variance is based on the covariance matrix estimated at each period of time, evaluating the relationships among the MNs, which enables to identify an anomaly. The prediction variance of a MN actually reflects its minimal degree of deviation with respect to the others of MNs.

By using prediction variance, cost is reduced. This results in high detection rate and improved performance.

Link quality: Link quality indicator is defined as the characterization of strength and/or the quality of a received packet. It is directly proportional to Received Signal Strength (RSSI). Its value varies from 0 to 255:

$$LQ \propto RSSI \tag{7}$$

RSSI is the ratio of the received Power (P_{rx}) to the reference Power (P_r) In general, P_r is equivalent to absoulte value say 1 mW:

$$RSSI = 10.\log \frac{P_{rx}}{P_{ref}} \text{ (dBm)} \tag{8}$$

When P_{rx} increases, then RSSI value is also increased which in turn enhances the link quality (Blumenthal *et al*., 2007).

Estimation of node coverage: The node Coverage (C_n) is estimated based on the relative node speed and node degree using Eq. (9):

$$C_n = (\alpha * z_i) + (\beta * D_{ni}) \tag{9}$$

where,
z_i = Relative speed of the node
D_{ni} = Node degree
α, β = Constants

In the above equation, z_i is determined based on the distance among the nodes at time t and the D_{ni} is related to the direct wireless link among the nodes at time t.

Cluster formation: The proposed technique involves the formation of cluster by dividing the network geographical area into equal groups. The following algorithm illustrates the formation of clusters.

Step 1: Each sensor node N_i deployed in the network broadcast the hello message to its neighboring nodes ($Neigh_i$):

$N_i \rightarrow Neigh_i$: Hello

The format of the Hello message is shown in the Table 1.

The parameters in the hello messages such as residual energy, link quality and node coverage are estimated in section estimation of metrics.

Step 2: Based on the Hello Message, each N_i identifies itself and also maintains the neighbors list (L_{neigh}).

Step 3: Based on the obtained parameter values, each node computes a weight value as follows:

$$W = w_1 * E_{res} + w_2 * LQ + w_3 * C_n \tag{10}$$

Where, w_1, w_2 and w_3 are weight factors.

Step 4:
If W is high
Then
N_i declares itself as CH immediately.
$N_i \rightarrow L_{neigh}$: CL_REQ
End if

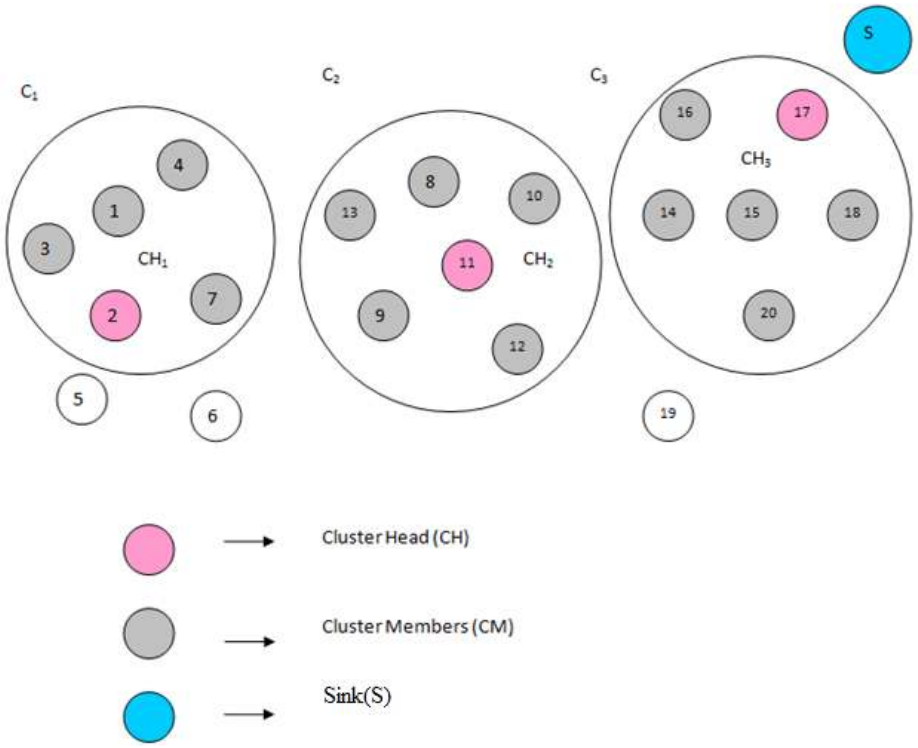

Fig. 1: Cluster architecture

The weight values is said to be high when E_{res}, LQ and C_n is greater than threshold value. Even if there is any lag in any one parameter threshold, then the node will get delayed in declaring itself as cluster head.

Step 5: Upon hearing the CL_REQ, the neighboring nodes in L_{Neigh} sends join reply message to N_i to join the cluster:

$N_i \leftarrow$ Lneigh: J_REP

Step 6: Following the cluster formation, the sink node (S_i) stores the details of all the CH's and their data structures and broadcast cluster information packet (C_IN) to all the CH's:

$S_i * \rightarrow$ CHs: C_IN

The C_IN includes the cluster heads ID and its position. CH's stores the C_IN in its cluster table.

Figure 1 describes the cluster formation architecture. The architecture includes the cluster members, cluster head and sink.

Fuzzy based anomaly intrusion detection system: We use fuzzy decision model to perform the intrusion detection. Initially, CH estimates the honest, energy level and unselfishness and prediction variance of each node. The four inputs, that is, honest, energy level and unselfishness and prediction variance are considered as the input for the fuzzy membership functions and based on the fuzzy rules, the optimal trust threshold is detected as output.

The steps that determine the fuzzy rule based interference are as follows.

Fuzzification: This involves obtaining the crisp inputs from the selected input variables and estimating the degree to which the inputs belong to each of the suitable fuzzy set.

Rule evaluation: The fuzzified inputs are taken and applied to the antecedents of the fuzzy rules. It is then applied to the consequent membership function.

Aggregation of the rule outputs: This involves merging of the output of all rules.

Defuzzification: The merged output of the aggregate output fuzzy set is the input for the defuzzification process and a single crisp number is obtained as output. The fuzzy inference system is illustrated using Fig. 2.

Fuzzification: This involves fuzzification of input variables such as Honest (H), Energy (E), Unselfishness (U) and prediction Variance (V) (Estimated in sections estimation of metrics) and these inputs are given a degree to appropriate fuzzy sets. The crisp inputs are combination of H, E, U and V. We take two possibilities, high and low for H, E, U and V.

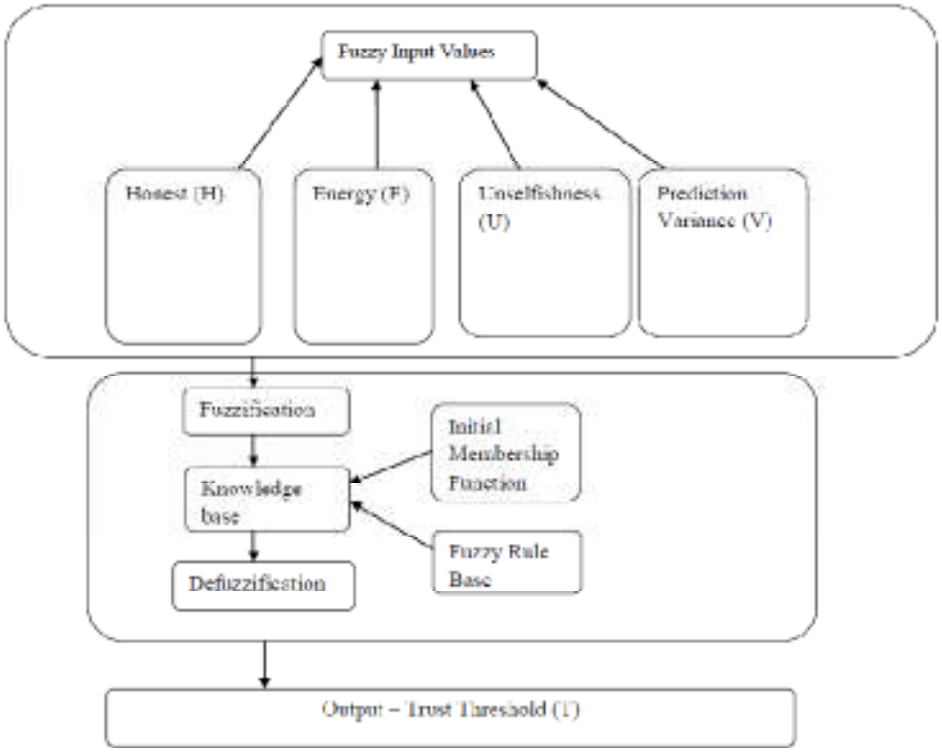

Fig. 2: Fuzzy interference system

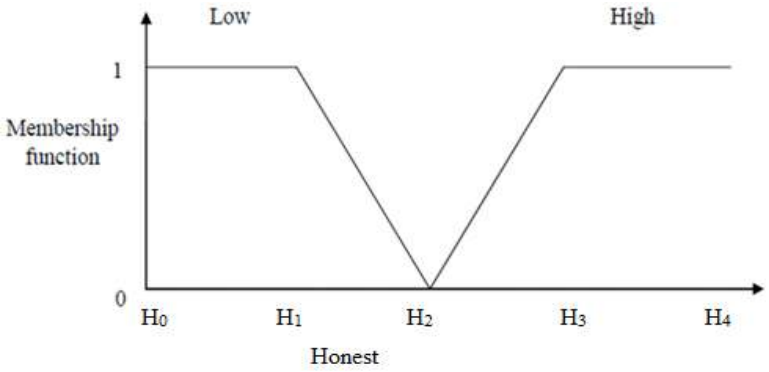

Fig. 3: Membership function of honest

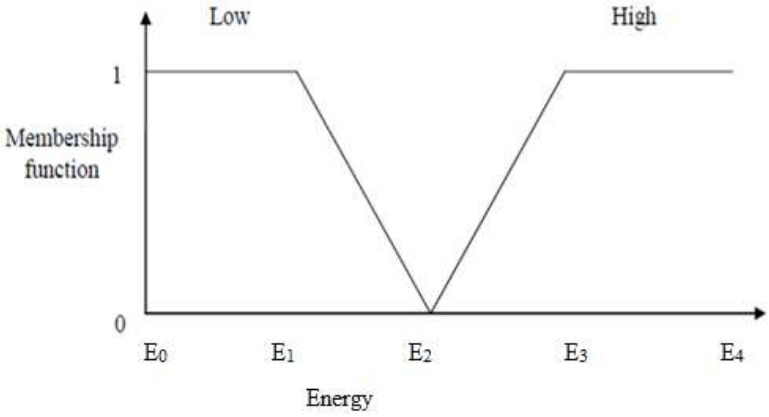

Fig. 4: Membership function of energy level

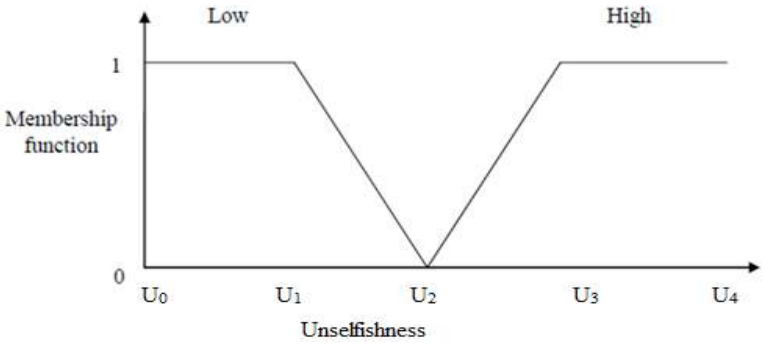

Fig. 5: Membership function of unselfishness

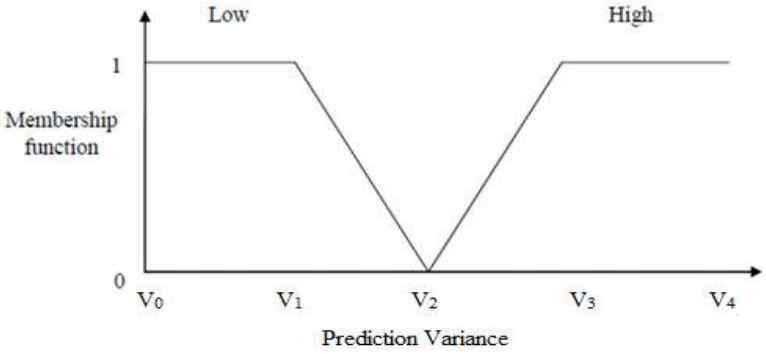

Fig. 6: Membership function of prediction variance

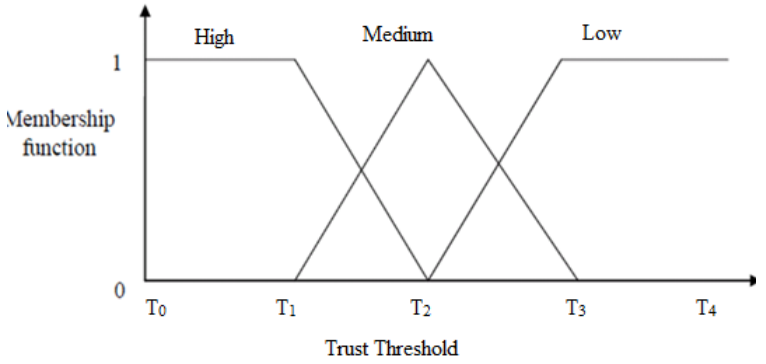

Fig. 7: Membership function of trust threshold

Figure 3 to 7 shows the membership function for the input and output variables. Due to the computational efficiency and uncomplicated formulas, the triangulation functions are utilized which are widely utilized in real-time applications. Also a positive impact is offered by this design of membership function.

In table H, E, U and V are given as inputs and the output represents the Trust Threshold (T). The fuzzy sets are defined with the combinations presented in Table 2.

Table 2 demonstrates the designed fuzzy inference system. This illustrates the function of the inference engine and method by which the outputs of each rule are combined to generate the fuzzy decision.

For example:

Table 2: Designed fuzzy inference system

H	E	U	V	T
Low	Low	Low	Low	Low
Low	Low	Low	High	Low
Low	Low	High	Low	Low
Low	Low	High	High	Low
Low	High	Low	Low	Low
Low	High	Low	High	Low
Low	High	High	Low	Medium
Low	High	High	High	Low
High	Low	Low	Low	Low
High	Low	Low	High	Low
High	Low	High	Low	Low
High	Low	High	High	Low
High	High	Low	Low	Medium
High	High	Low	High	Medium
High	High	High	Low	High
High	High	High	High	Medium

Let us consider Rule 16.
If (H, E, U = high and V= low)
Then
T = high
End if

This reveals that N_i contains the optimal trust threshold value.

Defuzzification: Defuzzification is used for extracting a crisp value from a fuzzy set as a representation value. We consider the centroid of area strategy for defuzzification:

$$F_{QoS} = \frac{\int_{f} \eta_{agg}(F)_{fdf}}{\eta_{agg}(F)_{df}} \quad (10)$$

where, $\eta_{agg}(F)$ = aggregated output of membership function.

RESULTS AND DISCUSSION

Simulation model and parameters: The Network Simulator (NS2, http:///www.isi.edu/nsnam/ns), is used to simulate the proposed architecture. In the simulation, 50 mobile nodes move in a 750×750 m region for 50 sec of simulation time. All nodes have the same transmission range of 250 m. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in Table 3.

Performance metrics: The proposed Fuzzy Based Anomaly Intrusion Detection System for clustered (FBAIDS) is compared with the Hierarchical Trust Management (HTM) protocol (Bao *et al*., 2012). The performance is evaluated mainly, according to the following metrics.

Packet delivery ratio: It is the ratio between the number of packets received and the number of packets sent.

Packet drop: It refers the average number of packets dropped during the transmission.

Energy consumption: It is the amount of energy consumed by the nodes to transmit the data packets to the receiver.

Delay: It is the amount of time taken by the nodes to transmit the data packets.

Detection rate: It is defined as the rate that the number of attacks can successfully be detected divided by the total number attacks performed.

Table 3: Simulation settings and parameters

No. of nodes	200
Area size	750×750
Mac	IEEE 802.11
Transmission range	250 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Rate	50 kb
Initial energy	14.3 J
Transmission power	0.660
Receiving power	0.395
Attackers	2, 4, 6, 8 and 10

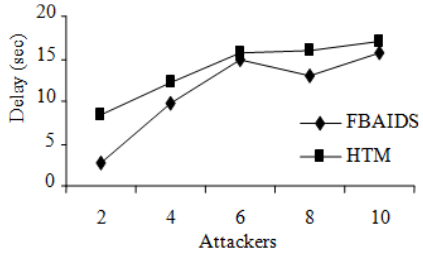

Fig. 8: Attackers vs. delay

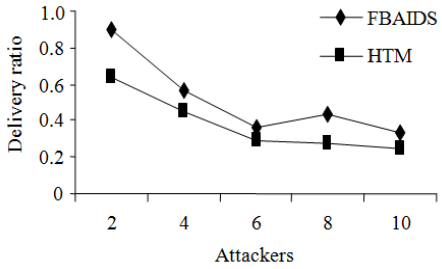

Fig. 9: Attackers vs. delivery ratio

False positive rate: If refers to the ratio of number of legitimate packets which are considered as malicious over the total packets sent.

Results: In the attack model, the Denial-of-Service (DoS) based attacks like flooding attack and false data injection attacks are considered. The number of attackers is increased from 2 to 10.

Figure 8 shows the delay of FBAIDS and HTM techniques for different number of attacker scenario. We can conclude that the delay of our proposed FBAIDS approach has 24% of less than HTM approach.

Figure 9 shows the delivery ratio of FBAIDS and HTM techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed FBAIDS approach has 27% of higher than HTM approach.

Figure 10 shows the drop of FBAIDS and HTM techniques for different number of attacker scenario. We can conclude that the drop of our proposed FBAIDS approach has 71% of less than HTM approach.

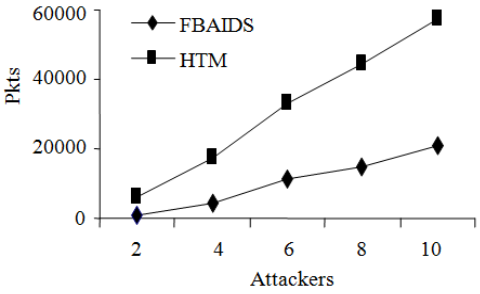

Fig. 10: Attackers vs. drop

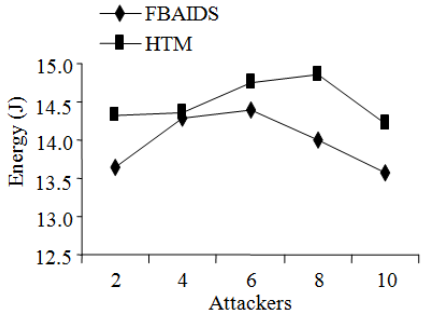

Fig. 11: Attackers vs. energy consumption

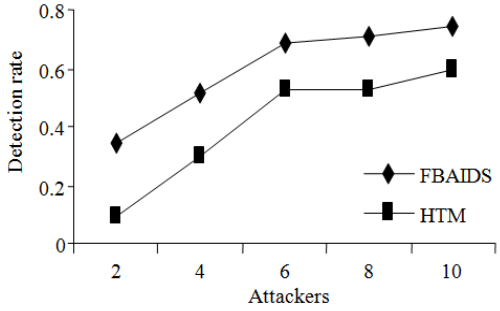

Fig. 12: Attackers vs. detection rate

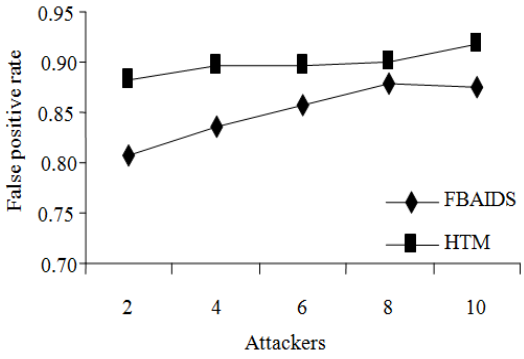

Fig. 13: Attackers vs. false positive rate

Figure 11 shows the energy consumption of FBAIDS and HTM techniques for different number of attacker scenario. We can conclude that the energy consumption of our proposed FBAIDS approach has 24% of less than HTM approach.

Figure 12 shows the detection rate consumption of FBAIDS and HTM techniques for different number of attacker scenario. We can conclude that the detection ratio consumption of our proposed FBAIDS approach has 37% of higher than HTM approach.

Figure 13 shows the false positive of FBAIDS and HTM techniques for different number of attacker scenario. We can conclude that the false positive of our proposed FBAIDS approach has 5% of less than HTM approach.

CONCLUSION

In this study, we have proposed a fuzzy based anomaly intrusion detection system for clustered WSN. Initially the cluster heads are selected based on the parameters such as link quality, residual energy and coverage. Then the anomaly intrusion is detected using fuzzy logic technique. This technique considers the parameters such as honest, energy level, unselfishness and prediction variance of each cluster member and provides the optimal trust threshold of the node as the result. By simulation result, we have shown that the proposed technique enhances the detection accuracy and reduces the false positive rate.

REFERENCES

Abduvaliyev, A., A.K. Pathan, J. Zhou, R. Roman and W. Wong, 2013. On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutorials, 15(3).

Bao, F., I. Chen, M. Chang and J. Cho, 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE T. Network Serv. Manage., 9(2).

Bhuse, V. and A. Gupta, 2006. Anomaly intrusion detection in wireless sensor networks. J. High Speed Netw., 15(1): 33-51.

Blumenthal, J., R. Grossmann, F. Golatowski and D. Timmermann, 2007. Weighted centroid localization in zigbee-based sensor networks. Proceeding of the IEEE International Symposium on Intelligent Signal Processing (WISP), pp: 1-6.

Coppolino, L., S. D'Antonio, A. Garofalo and L. Romano, 2013. Applying data mining techniques to intrusion detection in wireless sensor networks. Proceeding of the 8th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

Hsieh, C.F., Y. Huang and R. Chen, 2011. A light-weight ranger intrusion detection system on wireless sensor networks. Proceeding of the 5th International Conference on Genetic and Evolutionary Computing.

Jurdak, R., X.R. Wang, O. Obst and P. Valencia, 2011. Wireless sensor network anomalies: Diagnosis and detection strategies. Intell. Syst. Eng., 10: 309-325.

Li, Y., 2010. Anomaly detection in unknown environments using wireless sensor networks. Ph.D. Thesis, University of Tennessee.

Livani, M.A. and M. Abadi, 2010. Distributed PCA-based anomaly detection in wireless sensor networks. Proceeding of the International Conference for Internet Technology and Secured Transactions (ICITST).

Livani, M.A. and M. Abadi, 2011. A PCA-based distributed approach for intrusion detection in wireless sensor networks. Proceeding of the International Symposium on Computer Networks and Distributed Systems (CNDS).

Pugliese, M. and F. Santucci, 2013. The mean-variance estimator technique in monitoring applications using mobile agents over wireless sensor networks. Proceeding of the International Conference on MOBILe Wireless Middle WARE, Operating Systems and Applications.

Rassam, M.A., A. Zainal and M.A. Maarof, 2013. Advancements of data anomaly detection research in wireless sensor networks: A survey and open issues. Sensors, 13(8): 10087-10122.

Reznik, L., B.K. Bitemirov and M. Negnevitsky, 2009. Intrusion detection in sensor networks based on measurements. Proceeding of the IEEE Conference on SENSORS, pp: 1026-1029.

Riecker, M., A. Barroso, M. Hollick and S. Biedermann, 2012. On data-centric intrusion detection inwireless sensor networks. Proceeding of the IEEE International Conference on Green Computing and Communications and Conference on Internet of Things and Conference on Cyber, Physical and Social Computing.

Sedjelmaci, H., S.D. Senouci and M. Feham, 2012. Intrusion detection framework of cluster-based wireless sensor network. Proceeding of the IEEE Symposium on Computers and Communications (ISCC).

Stelte, B. and G.D. Rodosek, 2013. Thwarting attacks on ZigBee: Removal of the KillerBee stinger. Proceeding of the IFIP/IEEE International Conference on Network and Service Management (CNSM).

Sun, B., X. Shan, K. Wu and Y. Xiao, 2013. Anomaly detection based secure in-network aggregation for wireless sensor networks. IEEE Syst. J., 7(1).

Tiwari, M., K.V. Arya, R. Choudhari and K.S. Choudhary, 2009. Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information. Proceeding of the 4th International Conference on Computer Sciences and Convergence Information Technology.

Usman, M., V. Muthukkumarasamy, X. Wu and S. Khanum, 2012. Wireless smart home sensor networks: Mobile agent based anomaly detection. Proceeding of the IEEE 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp: 322-329.

Xiao, Z., C. Liu and C. Chen, 2009. An anomaly detection scheme based on machine learning for WSN. Proceeding of the 1st International Conference on Information Science and Engineering (ICISE).

Xie, M., J. Hu and S. Guo, 2015. Segment-based anomaly detection with approximated sample covariance matrix in wireless sensor networks. IEEE T. Parall. Distr., 26(2): 574-583.

Zhang, K., 2009. A danger model based anomaly detection method for wireless sensor networks. Proceeding of the 2nd International Symposium on Knowledge Acquisition and Modeling.

Zhao, R., X. Shen, Z. Jiang and H. Wang, 2012. Broadcasting with least redundancy in wireless sensor networks. Int. J. Distrib. Sens. N., 2012: 11.