International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Malicious Detection using Secure Mutual Trust Based Routing on an Intrusion Detection System in WSN

Abhishek Jain, Khushboo Tripathi

Abstract*: The Lack of infrastructure makes secured data distribution, challenging task in Wireless Sensor Networks (WSNs). In traditional routing methods, either security or routing optimization is addressed separately; however, both are not addressed at similar instances. Hence, if there exists a bottleneck while handling security or routing, where either one is affected by the other. In this paper, Mutual Trust Management (MTM) framework is designed between the sensor nodes is proposed in WSN to identify the malicious nodes. The trust model is connected with an Intrusion Detection System (IDS) to effectively analyse the malicious nodes and routing of packets between the nodes is designed with the Structure of a Multilayer Perceptron (MLP) Network to route the packets through the secured path. The simulations are conducted using the NS-2 setup for validating the trustworthiness and packet delivery through the secured route. The proposed method is compared against the existing methods to test the efficacy of MTM-MLP model and the results show that the MTM-MLP achieves higher detection against ransomware than the other methods.

Keywords: MLP, Mutual Trust, Routing, Security, WSN.

I. INTRODUCTION

WSN have unique characteristics that make them attractive for use in tough environments, which are otherwise not possible or difficult to operate [1]. WSNs, however, are subject to a number of security attacks, as any other type of network. For WSNs, security is a key topic. Compromised nodes could lead to misleading or inaccurate information, which could lead to a failure to achieve the network objective. Research was carried out to develop custom security methods for WSNs to determine privacy, integrity and availability. The security methods techniques can be classified as either preventive or detective [2]. The prevention is the first line of defense with low-overhead cryptography to ensure confidentiality, integrity and hashing methods [3]. The IDS detect the malicious interference in the network is the second line of defence. In addition, an IDS is classified according to its detection algorithm. In either the field of WSNs [4], numerous detection techniques were proposed. Some use methods of detection of misuse, but most use anomalies [5]. The anomaly detection method on the other hand detects further assaults and reduces the false negative rate. Offline training is necessary to determine the normal network conduct and the definition of some markers characterizing the normal conduct. When deployed, the activities of the network are compared to the preset threshold and all deviations from what are deemed normal are categorized as abnormal. Fixing thresholds too high might lead to high false negative alerts and high false positive alerts if the threshold is too low.
The malicious behavior is also defined in terms of network behavior, which is created by the malicious nodes to compromise the WSN objective. Attacks often target vulnerabilities in network layers. Ransomeware is one examples of network layer attacks, since it offer advantages over the vulnerabilities in a routing protocol. Apart from the network layer, it affects the network layers of local sensors [6]. We believe that the development of an IDS should take multi-layer monitoring and monitoring schemes into consideration.

A.Background

Ransomware attacks have been theorized back in 1996 and are now a reality. The files of the victim's device are encrypted by a typical ransomware and a ransom is asked for. The misconceived use a variety, simple and extremely effective extortion tactics. In the “best” case the device is locked but the information is left untouched; personal information is effectively encrypted in the worst possible case. Therefore, while it can somehow be removed, the victims have no choice but to pay for the requested ransom for their data to be restored [7] in the absence of a new backup.

Malware remains one of the major security threats on the Internet today. There has been a recent development of a specific malware form called ransomware among cybercriminals. From locks on the desktop of an infected machine to encrypt all its files, Ransomware operates in many different ways. Ransomware has behavioral differences in comparison to traditional malware. For instance, conventional malware usually strives for stealth so that it can collect credentials or keystrokes without increasing suspicion. Ransomware, by contrast, are directly opposed to stealth, because the whole point is to inform the user that they are infected [8], where the attacks are not possible.

Manuscript published on 30 September 2019
* Correspondence Author
Abhishek Jain*, department, Amity University, Gurgaon, India. Email: abhishekjain_25@yahoo.co.in
Dr. Khushboo Tripathi, department, Amity University, Gurgaon, India. Email: ktripathi@ggn.amity.ed

Ransomware uses a number of detection, propagation and attacking strategies, like other classes of malware.

Persistent desktop message. The malicious program typically gives the victim a message after successfully performing a ransomware infection. This “random note” tells users that their computer has been “locked” and gives instructions on how to restore access to a ransom payment. You can generate this Ransom message in various manners. One popular technique is to call up dedicated API functions to create a new desktop and to lock the victim out of the affected system by default. Malware writers can also use HTML to view this message or create other forms of persistent windows. Show an ongoing desktop message in many ransomware attacks is a classic action.

Indiscriminate actions on files. A ransomware attack in a crypto-style lists the victims ' files and encrypts any private files they find aggressively. By retaining the decryption clave, access is restricted. The malware on the victim's computer, or the remote servers on the server, can create encryption keys, and then be sent to the compromise computer. An attacker may use custom destructive functions, or delete the original user's files with Windows API features. The attacker is also able to overwrite the encrypted version of the files by using the Secure Deletion API of Windows.

Selective actions on files using attributes. A large number of ransomware samples selectively encrypt a private user file to avoid detection. The ransomware sample can list the files based on the access date in the simplest form. The malware could also open the application and list the files that have been recently reached in more sophisticated scenarios. In order to get this type of information, the sample can also inject malicious code into any Windows application.

In this paper, Mutual Trust Management (MTM) framework is designed between the sensor nodes is proposed in WSN to identify the malicious nodes. The trust model is connected with an Intrusion Detection system to effectively analyse the malicious nodes and routing of packets between the nodes is designed with the Structure of a Multilayer Perceptron (MLP) Network to route the packets through the secured path.

The outline of the paper is given below: Section 2 discusses the related works. Section 3 provides the details of the proposed method. Section 4 evaluates the proposed work with other existing models. Section 5 concludes the paper.

II. RELATED WORKS

In order to better detect and classify four types, Almomani, I., et al. (2016) [10] have developed a special data set for WSN: black hole, gray hole, flooding, and scheduling attacks. The application of LEACH, the most famously used hierarchical routing protocol on WSNs, is considered in this method. That is because LEACH is one of the most popular hierarchical routing protocols on WSNs, with low energy consumption and its simplicity. The built-in data set is known as WSN-DS.

Pathak, V., et al. (2017) [11] has proposed a Multi-level Probabilistic Sensing Model TMSM (Tunable Multilevel Probabilistic Sensing Model) which has more sensing rank than Boolean sensing models. This study incorporated the TMSM into the Gaussian distributed network.

Selvakumar, K., et al. (2019) [12] proposed a Fuzzy Rough attribute selection adaptive IDS based on Allen's algebra interval and an extensive number for WSN attack prediction [12]. The IDS was applied to network trace datasets. In addition, efficient classification of the network trace data set has been proposed for an innovative and roughly based neighbourhood algorithm.

Meng, W., et al. (2017) [13] proposed a combination of the hierarchical structure of the Bayesian trust management for intrusion detection with traffic sampling. Jin, X., et al. (2017) have developed a multi-agent model framework for intrusion detection in both the cluster heads and the common sensor nodes. The first is to define different typical trust characteristics of the node, and the Mahalanobis theory is applied to determine the normality. Secondly, based on the combination of beta distribution and a tolerance factor, the trust value of the node is calculated and modernized.

Numerous approaches and schemes discussed here and in other research articles aimed at improving the routing process and maintaining confidence-based communication through ad hoc multi-hop network services. Others aim to prevent certain security attacks from protecting the routing procedure. As these improvements address the trust problem, they all have certain weaknesses, which either affect the overall performance or increase overall costs considerably.

2. Proposed Method

In this section, Mutual Trust Management (MTM) framework is designed between the sensor nodes is proposed in WSN to identify the malicious nodes. The trust model is connected with an Intrusion Detection system to effectively analyse the malicious nodes and routing of packets between the nodes is designed with the Structure of a Multilayer Perceptron (MLP) Network to route the packets through the secured path.

A.Network Topology

Implementing layer-cluster topology results in increased scalability while efficiently reducing a network's management complexity and communication costs. The topology of WSNs is, therefore, cluster-based for most practical applications. As shown in Fig. 1, the network of layer-clusters includes ordinary SNs, CH and a base station (BS), which is considered in this paper. SNs have restricted energy supply, computing, storage, communication and other capabilities. Communications between the SNs and the CHs is done with a single hop, while the SNs and the BS communicate through CHs. The CHs can communicate with the BS either on a single-stop or multi-hop basis. The CHs manage the nodes in each cluster and need more energy, memory, and computing than the SNs because they are required to perform more tasks.

Retrieval Number: C5003098319/2019©BEIESP
DOI:10.35940/ijrte.C5003.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

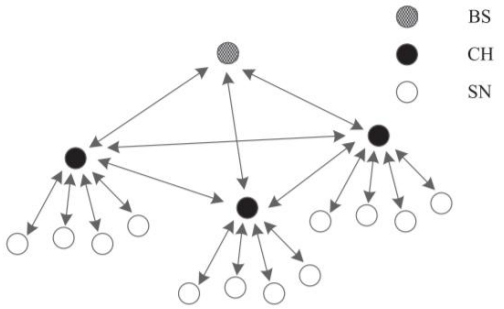

Fig. 1. Network topology structure

B. Mathematical model

The study designs a system for modelling the immune system response, malicious object interaction and the relative characteristic of the damaged nodes. It is supposed to follow a dynamic model with malicious object detection. The development of the malicious intruders depends entirely on the initial condition and the effect it produces over time, whereas immune response changes depends entirely on its initial condition. Finally, the malicious object density and its degeneracy depend on the relative characteristics of the damaged nodes. The following system of differential equations may then regulate the dynamic of the system:

$$\frac{dP}{dt} = \beta P - \gamma IP - \beta_0 P^2$$

$$\frac{dI}{dt} = \mu - aI - bIP - \eta\gamma IP$$

$$\frac{dM}{dt} = \alpha P - \alpha_0 M$$

$$I(0) \geq 0, M(0) \geq 0, P(0) \geq 0, 0 \leq \eta \leq 1$$

Here,

$I(t)$ - system immune status,

$P(t)$ - malicious object density,

$M(t)$ - damaged node relative characteristic at time $t \geq 0$.

β - malicious object growth rate coefficient,

γ - malicious object decay rate coefficient and its interaction with network immune system

b_0 - malicious objects intraspecific interference coefficient.

l - immune system growth rate,

α - natural decay rate coefficient,

b - immune system stimulating growth rate and its malicious objects interaction,

g - decay rate coefficient and its malicious objects interaction,

a - damaged malicious node growth rate coefficient and

a_0 - natural decay rate coefficient [15].

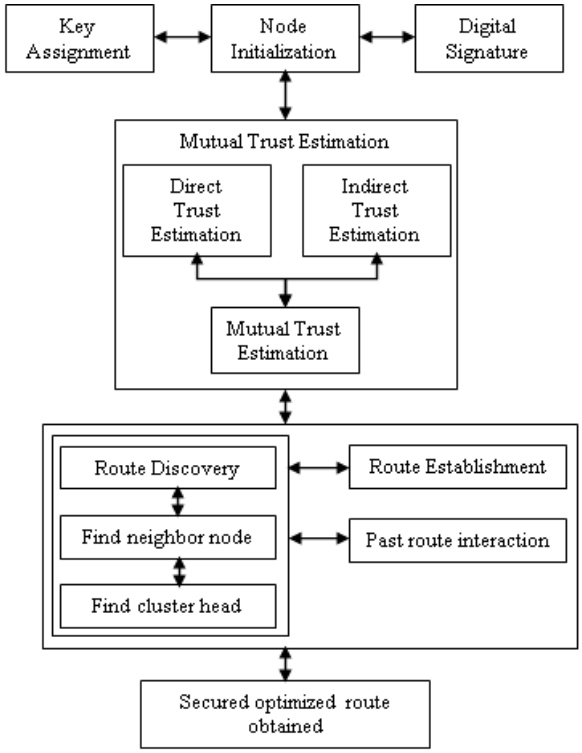

Fig. 2. Architecture of MTM-MLP.

C. MTM to estimate Genuine Nodes

This section discusses the trust relationship between the sensor nodes. The mutual trust between the sensor nodes is estimated based on direct trust and indirect trust.

The trust value in WSN, say G is calculated between nodes u and v. Initially, the nodes u and v are justified in terms of its nodes that are adjacent. If the node u is adjacent to node v, then the trust value between nodes u and v is the direct trust $d(u,v)$. If the node u is not adjacent with node v, then the trust value between u and v is estimated as indirect trust model $i(u,v)$. Finally, the trust $t(u,v)$ between u and v are figured out. Similarly, the trust $t(v,u)$ between the nodes v and u are calculated in same manner. A comparison between the trust $t(u,v)$ and the trust $t(v,u)$ are made in order to find the mutual trust.

i. Direct Trust

The direct trust model is estimated in terms of communication of nodes, active cooperation of nodes and association of nodes with network to a certain degree, which defines the extent of trust. This direct trust offers subjective relationship between the sensor nodes that considers subjective actions. Here, the analysis of direct trust degree is carried out in detail using similarity and tie strength of nodes. Similarly, analysis of indirect trust degree is carried out using distance between the nodes. The direct trust relation in terms of tie strength is shown in Definition 1 and direct trust relation in terms of similarity between nodes is shown in Definition 2.

***Definition* 1**: To an adjacent node pair, the strength of tie between sensor nodes is used to find the trust, which forms the direct trust and its degree is calculated as,

$$d_r(u,v)=\frac{w(u,v)}{w(u)}, \text{where } d_r(u,v)\in(0,1] \quad (1)$$

where $d(u,v)$ defines the direct trust degree between the nodes u and v. $w(u,v)$ defines the node strength. $w(u)$ defines the total tie strength of node u and neighboring node other than node v. $w(u,v)$ is also referred as collaborative or interactive number among the nodes in network.

There always exist a homogeneity among nodes in network i.e. similar nodes are correlated between one another. The similarity of node is estimated by measuring the total shared neighbors between neighbor nodes. When the nodes similarity is high, the neighboring nodes tends to overlap each other at a larger extent. Hence, the present node contributes a very less similarity over a larger number of neighboring node.

***Definition* 2**: To an adjacent node pair, the sensor node similarity is used to find the direct similarity trust, which is calculated as,

$$d_s(u,v)=\sum_{t\in N(u)\in N(v)}\left(I(t)\right)^{-1} \quad (2)$$

where $d_s(u,v)$ defines the direct trust degree using node similarity. The neighboring set of u and v is $N(u)$ and $N(v)$, respectively to estimate the similarity of nodes. $I(t)$ defines the penetration degree of t.

Finally, the direct trust between the adjacent nodes u and v is given as,

$$d(u,v)=d_r(u,v)+d_s(u,v). \quad (3)$$

ii. Indirect Trust

Indirect trust considers the transmission of information between the sensor nodes.

The indirect connections exist due to non-adjacent nodes opens up connections via intermediate nodes. This leads to creation of indirect trust between the nodes that are nonadjacent to each other, which is estimated via direct trust between the adjacent nodes. The transmission trust between source and target node takes different form, namely, single and multi-path method. The indirect trust using single path method is given in definition 3 and indirect trust using multi path method is given in definition 4.

***Definition* 3**: To a non-adjacent source (u) and target node (v) with a single transmission path between them forms an indirect trust of single path. The approachable path between the non-adjacent nodes are constructed in terms of intermediate relationship between the nodes u and v. The indirect trust of single path is thus estimated as follows:

$$i_s(u,v)=\begin{cases} mt\dfrac{d_{\max}-d_{u,v}+1}{d_{\max}} & \text{if } d_{u,v}\le d_{\max} \\ 0 & \text{if } d_{u,v}>d_{\max} \end{cases} \quad (4)$$

where, $mt = \min(d(u, u_1), d(u_1,u_2),\cdots, d(u_n,v))$, which forms the intermediate route length between the nodes u and v and d_{max} defines the trust transmission with maximum distance. The theories suggests that as the transmission distance increases, the integrity and accuracy of information tends to reduce.

***Definition* 4**: To a non-adjacent source (u) and target node (v) with two approachable transmission path between them forms an indirect trust of multi-path. The indirect trust of multi-paths obtains maximal value after the estimated, which is stated as follows:

$$i_m(u,v)=\max_{paths(u,v)}\{i_s(u,v)\} \quad (5)$$

where $i_m(u,v)$ defines the degree of indirect trust in multi-path between node u and node v. The path set between the node u and node v is given by $paths(u,v)$. Hence, the trust degree between the node u and node v in the network G is given as,

$$t(u,v)=\begin{cases} d(u,v) & \text{if nodes are adjacent} \\ i_m(u,v) & \text{else} \end{cases} \quad (6)$$

iii. Mutual Trust

The trust value is estimated between the nodes using direct trust and indirect trust model. The trust between the nodes pairs is always not similar i.e. $t(u,v) \neq t(v,u)$ and this is justified as the node with directional property. Additionally, the presence of malicious nodes may not send a response to the node, which has sent a message. This creates an unusual behavior on adjacent sensor nodes i.e. disparity in trust. This has a negative influence over accuracy on trust-based detection. Hence, non-directional model is required to create mutual trust between nodes u and v and nodes v and u.

***Definition* 5**: A non-directional reciprocal trust between adjacent nodes u and v is called as mutual trust. The mutual trust is computed, when the $T(u,v)$ = {trust(u,v), trust(v,u)}, which is given as follows:

$$m(u,v)=\begin{cases} \min\left(T(u,v)\right) & \text{if } \min\left(T(u,v)\right)\ge\chi \\ 0 & else \end{cases} \quad (7)$$

where $m(u,v)$ defines the mutual trust between node u and node v, χ defines the degree of trust tolerance to control the minimum allowed level of trust in a network.

The conversion of node trust into mutual trust resolves unusual behavior of nodes and reduces the constraints associated with detecting the trust levels with increased accuracy.

D.MLP for Routing

MLP belongs to the neural network supervised class of networks and is one of the most widely used NN in IDS. There are three layers of nodes for processing in MLP network i.e an input layer, hidden layers and the outgoing layer (Fig. 3).

The neural network principle is that the net neurons perform hidden layers calculations when data are accessible on the input layer, until an output value is achieved at each output neuron. This output indication should be able to indicate the appropriate input data class. That means, on the right neuron and on the remaining low output values you can expect high output value. An artificial neuron node in the MLP is as shown in Fig. 4, which calculates the weighted sum of the inputs with bias and transfers that sum values through the activation function.

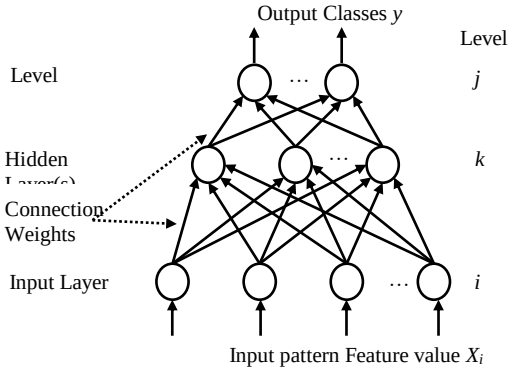

Fig. 3. Structure of a MLP.

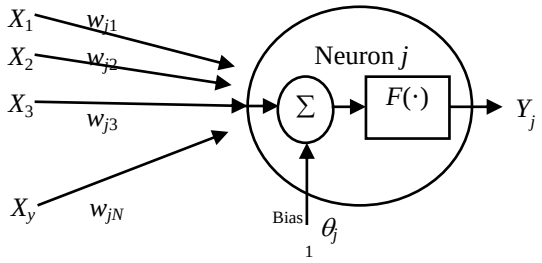

Fig. 4. One node of MLP.

The process of MLP is defined:

$$V_j = \sum_{i=1}^{p} W_{ji} X_i + \theta_i \quad (1)$$

$$y_i = f_j(V_j) \quad (2)$$

where,

V_j - input linear combination X_1, X_2.

X_p – bias, which is the connection weight between a neuron j and an input

$f_i(\cdot)$ - j^{th} neuron activation function

y_i - output.

The sigmoid activation function is defined as.

$$F(\alpha) = \frac{1}{1+e^{-\alpha}} \quad (3)$$

The training and testing phase are part of any network. This training stage is based on the learning algorithm for updating the weight value of the network. The weights of the neural network are updated by the most frequently used algorithm Back Propagation (BP), according to Eq.(3) in a monitored mode.

$$W_{ij}(t+1) = W_{ji}(t) - \varepsilon \frac{\delta E_f}{\delta W_{ji}} \quad (4)$$

where, ε - learning rate and E_f - error function.

For each input training pattern, during the learning stage the output of the forward neural feed networks is calculated. To update the weight of the network through back propagation algorithm, the error between computed and the desired output is used.

E. Routing Framework

This paper proposes to expand the AODV on-demand routing protocol in the MLP protocol. MLP Protocol modifies the Routing Request Frame (RREQ) and the Routing Answer Frame (RREP) of the MLP Protocol in order to find a secure and energy-efficient route by adding the information about MLP's trust and route prediction. Without increased communication traffic, we can exchange trust and energy information. The MLP protocol defines the path-complete cost PCC, and a better forwarding path can be compared with the PCC by the data source node. Comprehensive path costs PCC takes into account the trust value, the rest of the energy and the hop count; and PCC can be calculated as follows:

$$PCC = w_t \cdot \sum_{i=1}^{n}(1 - MTM_i) + w_e \cdot \sum_{i=1}^{n}(1 - E_i) + w_{hop} \cdot Count_{hop} \quad (5)$$

where, w_t, w_e and w_{hop} - coefficients of trust weight, coefficients of residual energy and coefficients of hop count, respectively and $w_t + w_e + w_{hop} = 1$.

In this paper, we allow the three coefficients to be equal for confidence, energy and hops. The coefficients can be adjusted to meet actual demands.

III. Results and Discussions

We show the MTM-MLP operations in this section and evaluate the overall performance. To generate a test case and measure results using the MTM-MLP protocol, a simulation environment for an ad hoc network was used. Table 1 presents the simulation parameters.

Table- II: Simulation Parameters

Parameters	Value
Total number of Nodes	50
Transmission Range	250m
MAC layer	802.11
Area Size	1200 × 1200m^2
Packet Size	512 bytes
Mobility Model	Random Way Point
Total Simulation Time	75 sec
Traffic Source	CBR (UDP)
Propagation mode	Free space
Maximum connection	10
Operating Frequency	2.4GHz
Movement speed	1 ms^{-1}
Simulation time	75s
Type of attack	Ransomware

The proposed metric is evaluated using following metrics, which is shown below: end-to-end delay, control overhead, data reliability, node reliability, packet integrity and residual energy.

F. Dataset

The data set is probably the most important, but often overlooked task in designing a prediction model. The dataset should be fully representative of the target population if constructed correctly to ensure that the model is training in examples expected in real-world applications. This is easier said than done for classification tasks, like ransomware, where the target population includes an almost endless and constantly growing software collection–benign and ransomware [9]. For a representative collection of ransomware samples, it is not so much a question of quantities but of variety-training on 1000 Locky samples should be no more useful than training on one Locky sample for a noise-insensitive prediction model.

Ransomware prediction model has been trained on around 300 unique families and variations of ransomware. Each ransomware model was analyzed carefully and labeled by family and variant manually in the training pack, to ensure that the ransomware was represented in a balanced interior. Synthesising techniques were used to synthesize "future" ransomware behaviour, to further increase the variability in training set [9].

The benign dataset is a reference point to the ransomware and is therefore as important as the ransomware dataset. A real-life office of computers with data collectors collected the bulk of benign performance products used in Ransomware training [9].

G. Results

The proposed system is compared with other existing methods like: LEACH IDS [10], MLPSM IDS [11], Fuzzy IDS [12] and Bayesian trust IDS [13]. The Fig. 5 shows the data reliability, where the proposed system achieves higher reliability than the existing methods. The Fig. 6 shows the control overhead results, where the proposed method achieves reduced rate than other methods. The Fig.

7 shows the end to end delay, where the proposed method has reduced delay, where in Fig. 8, the residual energy of the proposed method, the node reliability in Fig. 9 and packet integrity in Fig. 10 has higher rate than the other methods. These results show that the proposed method is effective in detecting the ransomware than the other methods.

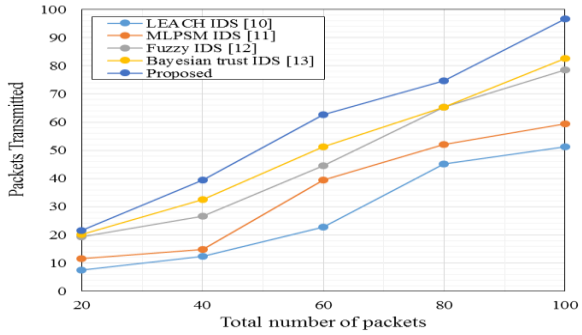

Fig. 5. Data reliability.

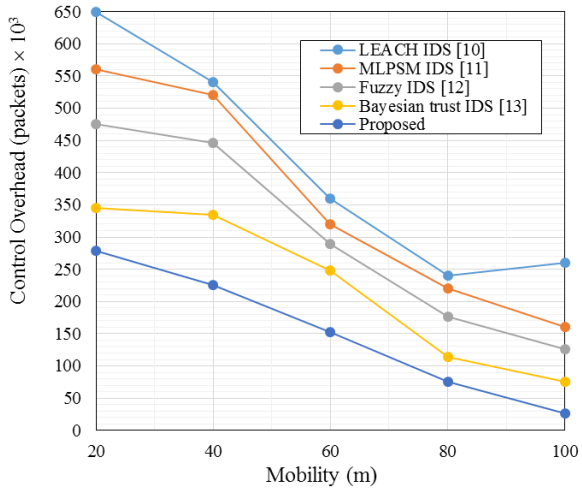

Fig. 6. Control overhead.

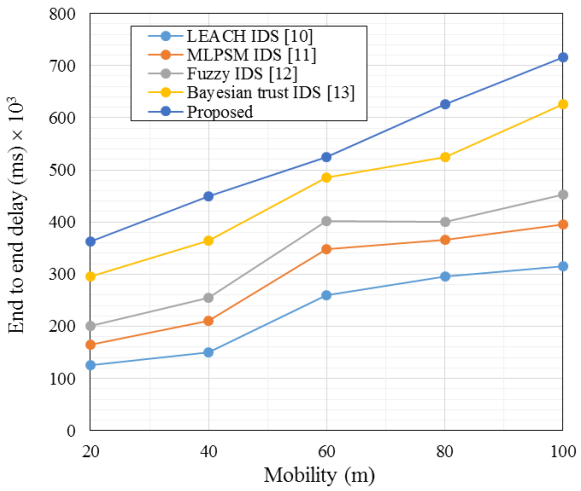

Fig. 7. End to End delay.

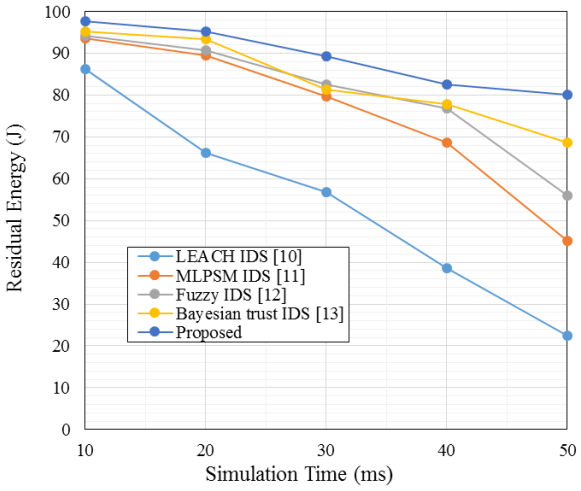

Fig. 8. Residual energy.

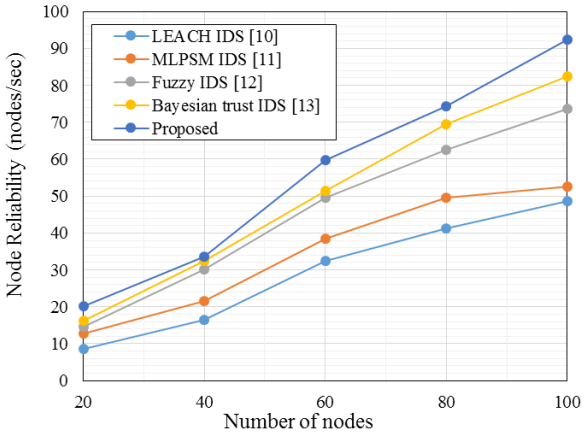

Fig. 9. Node reliability.

Retrieval Number: C5003098319/2019©BEIESP
DOI:10.35940/ijrte.C5003.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

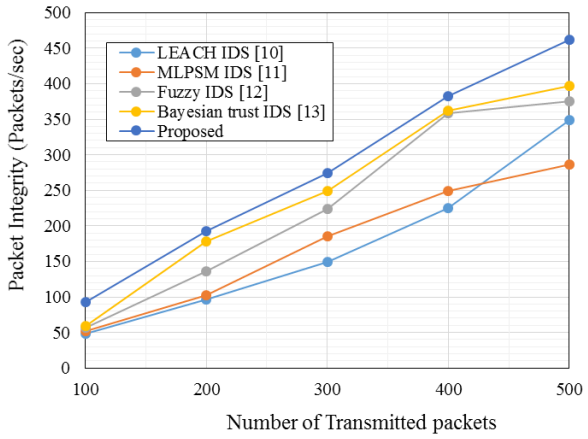

Fig. 10. Packet Integrity.

IV. CONCLUSIONS

In this paper, an MTM framework is designed between the sensor nodes is proposed in WSN to identify the malicious nodes. The trust model is connected with an Intrusion Detection system to effectively analyse the malicious nodes influenced by ransomware behavior and routing of packets between the nodes is designed with the MLP Network to route the packets through the secured path.

The simulations validates the trustworthiness and packet delivery through the secured route. The proposed method is compared against the existing methods to test the efficacy of MTM-MLP model and the results show that the MTM-MLP achieves higher detection against ransomware than the other methods.

REFERENCES

1. G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
3. H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.
4. B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
5. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
6. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," IEEE J. Quantum Electron., submitted for publication.
7. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
8. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].
9. M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.
10. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). Title (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)
11. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
12. (Journal Online Sources style) K. Author. (year, month). Title. Journal [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)

AUTHORS PROFILE

Abhishek Jain received the Bachelor of technology in from Guru Jambheshwar University of Science & Technology, and Master of Technology from Maharshi Dayanand University Rohtak. Currently He is pursuing PhD in the Department of Computer Science and Engineering, Amity University Haryana, India. He is expert in cyber forensics and research interests include protection from cyber attacks

Dr. Khushboo Tripathi is currently Assistant Professor at Amity University Haryana in Computer Science department.