International Journal of Engineering & Technology, 7 (4.20) (2018) 15-21

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Multi-dimensional trust aware routing for clustered IOT framework

Ashwala Mohan[1*], Dr. Bhanu Bhaskara[2]

[1*]*Research Scholar, Department of ECE, Rayalaseema University, Kurnool, Andhra Pradesh, India*
[2]*Professor, College of Computer and Information Sciences, Majmaah University, Saudi Arabia*
**Corresponding author E-mail:*ashwala@yahoo.com

Abstract

With the increased interest in the utilization of smart applications, the IoT has gained a lot of popularity in the real world scenario. Due to the integration of different heterogeneous devices in a single network, various types of security issues will arise in the IoT. To ensure more security in IoT, this paper proposes a new trust aware routing framework based on the inherent communication and data properties of devices connected in the network. A new trust metric is derived in this paper by combining two different trusts based on the communication between nodes and the information passing through them. Further to achieve a prolonged network lifetime with optimal resource conservation, a clustering based communication strategy is accomplished. Extensive simulations are carried out by varying the malicious nature of network and the performance is measured through the metrics, packet loss ratio, packet delivery ratio, delay, network lifetime and average energy consumption.

Keywords: *IoT, Trust, Social Trust, Information Trust, Packet Delivery Ratio, Network Lifetime*

1. Introduction

With several billion devices being connected in the last few years, the Internet of Things (IoT) is one of the most emerging technologies in computer science. There are a lot of applications that have been realized using IoT networks. Like all networked systems, the IoT based projects are subject to malicious attacks that can be quite serious due to its ubiquitous use in our daily life. From a logical viewpoint, an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfill a common goal. At the technological floor, IoT deployments may adopt different processing and communication architectures, technologies, and design methodologies, based on their target. For instance, the same IoT system could leverage the capabilities of a wireless sensor network (WSN) that collects the environmental information in a given area and a set of smart phones on top of which monitoring applications run. In the middle, a standardized or proprietary middleware could be employed to ease the access to virtualized resources and services. The middleware, in turn, might be implemented using cloud technologies, centralized overlays, or peer to peer systems [1].

Due to the high level of heterogeneity, there is a possibility of magnification of various security threats of the present internet which are being increasingly used to let interact machines, robots, and humans, in any combination. One of the main features is to have secure communication across the network. This holds particularly since many of the devices are small and have significant limitations with respect to memory, processing power, energy consumption, and bandwidth [2]. Therefore, many traditional security mechanisms cannot be used. Simultaneously, it is mandatory to develop a trust, privacy and valid security model to get an acceptance by users in the context of IoT applications [3-5]. With reference to security provision, data confidentiality, anonymity and integrity needs to be ensured, as well as authorization and authentication mechanism to stop the unauthorized users (i.e., devices and humans) from accessing the system. Whereas, regarding the requirement of privacy, both the confidentiality of user’s personal information and data protection have to be ensured, since the devices may manage sensitive information.

Trust management is one of the security ensuring strategies to provide data protection and also the confidentiality of user’s personal information. Trust based security provision involves the evaluation of trustworthiness of devices which are in the IoT network and asks for help by other devices. The device which seeks the help measures the trustworthiness of its neighbour devices before forwarding data through it. The main problem with approaches towards defining the trust is that they do not lend themselves to the establishment of metrics and evaluation methodologies. Moreover, the satisfaction or trust requirements are strictly related to the identity management and access control issues.

This paper develops a new trust based framework for IoT to achieve a more effective data confidentiality, integrity and availability. The proposed trust framework measures the trustworthiness based on the functional behavior of neighbour devices. Two types of trusts, namely social trust (ST) and information trust (IT) are proposed here and by combining these two metrics, a composite metrics is proposed which helps in the route establishment between IoT devices. . Simulation experiments are conducted over the proposed method with varying malicious rate and the performance is measured through the packet loss ratio, packet delivery ratio, delay, network lifetime and average energy consumption.

Rest of the paper is organized as follows: section-2 illustrates the details of literature survey. Section-3 illustrates the details of proposed approach. Experimental results are illustrated in section-4 and finally conclusions are described in section-5.

2. Literature Survey

Various approaches are proposed earlier to ensure the trust between the nodes communicating in the IoT network. A Secure Routing Protocol Based on RPL protocol is proposed in [6] to minimize the rank manipulation impact using the concept of rank threshold limits and hash chain authentication. However this protocol uses cryptography with hash chain authentication, which is computationally expensive. In [7], a trust-based design is developed to perform Rank falsification attacks in RPL. Here the node's behaviour and the trust along a path are used in determining a secure and optimal routing path. However there is no simulation to validate the proposed design. To detect RPL rank inconsistencies, a low false alarm RPL network monitoring system is developed in [8] based on the inconsistencies in the time-stamps of routing paths. However it does not provide a system to guard against the falsification of the time-stamp by malicious nodes.

A secure smart grid communication system using encrypted authentication system is developed in [9] to detect Sinkhole and distance spoofing attacks. Here the Cryptography and data mining techniques are utilized to detect the key-compromising node. However it is unable to detect anomalous requests from compromised nodes in the network that can be used to perpetrate attacks. A probabilistic constraint based specification model of an intrusion detection response system is developed in [10] to defend against Sinkhole attacks in RPL networks based on statistical probability. However it is prone to many false positive alerts and energy node depletion. A specification-based Intrusion Detection System (IDS) is proposed for detecting attacks on RPL-based network topology in [11]. It detects Rank, Sinkhole, Local Repair, Neighbour, and DIS attacks. Although detects them it does not isolate malicious nodes from the network. However this method is prone to high false positive alerts and also, high energy consumption as the number of nodes increases. Further an intrusion detection system that uses node location, received signal strength, and neighbour node information to detect Wormhole attacks is developed in [12]. It requires strategic placement for efficient detection. In a mobile environment, this will prove ineffective against attackers. Energy overhead also increases as the number of nodes increases.

A distributed trust management approach is proposed in [16] which computes the trustworthiness of nodes locally. Based on the service availability of nodes, the trust is defined here through the direct observation. This method consumes more time and resources. It requires approximately 120 minutes to complete the local table with complete trusted and malicious nodes. Moreover this method didn’t consider the initial trust level of a peer node. Recently, a study in [14] introduced a punishment and reward mechanism to protect the OA menace in IoT network. Further an adaptive security model was proposed in [17] considering three basic facts such as recommendations, observations and experiences. It focused on the reduction of energy consumption in the mobile Adhoc Network. A clustering based trust mechanism is proposed in [18] which addresses the security problems in IoT. It finds the similarity of interest in every cluster through the Kalman filter to estimate the trust value in advance.

A reinforcement learning mechanism is proposed in [19] which builds a feedback system on the trust which is based on loading method for mobile to mobile communications. For every interaction from the initiator node to the other nodes, the trust levels are evaluated to make it to perform more securely in further interactions. The main focus of this method is the trust by which most of the energy will be consumed and computational speed of device by which the communication speed will improve. However, this approach does not consider the trustworthiness of the data collected at every node. A trustworthy and secure sensing scheme is proposed in [20] based on the real alert policy. In this scheme, the trust evaluation considers the anomalous data and contextual information which represents the environment from which the anomalous data was acquired. The policy rule defines the trust evaluation mechanism under different situations. For an outdated policy, a new device or a new abnormal observation is considered as an attacker or malicious.

A multidimensional trust evaluation model is suggested in [21] in which the direct trust value is measured form the network communication. Under multidimensional trust, the delay, consistency of packet content, repetition rate, packet forwarding capacity, and integrity rate are measured through the D-S theory. However as the number of devices increases, the evaluation of multidimensional trust at every node results in more delay and continuously streaming data is complex to manage with conventional network communication analysis methods. A trust relationship based trust evaluation is proposed for clustered WSN in [22]. The trust relationship considers the message, communication, energy factors for each trust factor to detect the attacks.

3. Proposed approach

The proposed trust-aware security framework for IoT is illustrated in this section. Considering the resource constraints of nodes in IoT, this paper proposed a new energy efficient trust evaluation strategy by which the network lifetime and the security can be achieved simultaneously. For this purpose, this framework applied a trust based strategy in which a node is communicated with next hop node after knowing its trustworthiness only. The trustworthiness of a node is evaluated in two stages, one through direct evaluation, called as direct trust and another through indirect evaluation, called as recommended trust. The direct trust evaluation and indirect trust evaluation belongs to the network related issues. To obtain more clarity over the trustworthiness of next hop node, this approach further considered the Information related trust or content trust. Further to enhance the network lifetime the complete trust evaluation process is done by cluster heads only for every cluster.

3.1 Clustering of network

Here the nodes in the IoT network are formulated into different clusters and every cluster composes of nodes and one cluster head. The cluster head is selected based on the resource richness, i.e., the node which has more energy is considered as cluster head. The trust evaluation process is completely carried out through the cluster head only. The members of IoT are categorized as nodes (Ns), and Cluster Heads (CHs). In every cluster, the CH receives information from every IoT nodes and forwards to next cluster head [11], [12]. In the distant communications, the cluster head seeks the help of remaining cluster heads to transmit the data to the destination node. This is called multi-hop routing. In every cluster each node has one unique identity and belongs to only one cluster. Figure.1 represents the formulation of clustering the network.

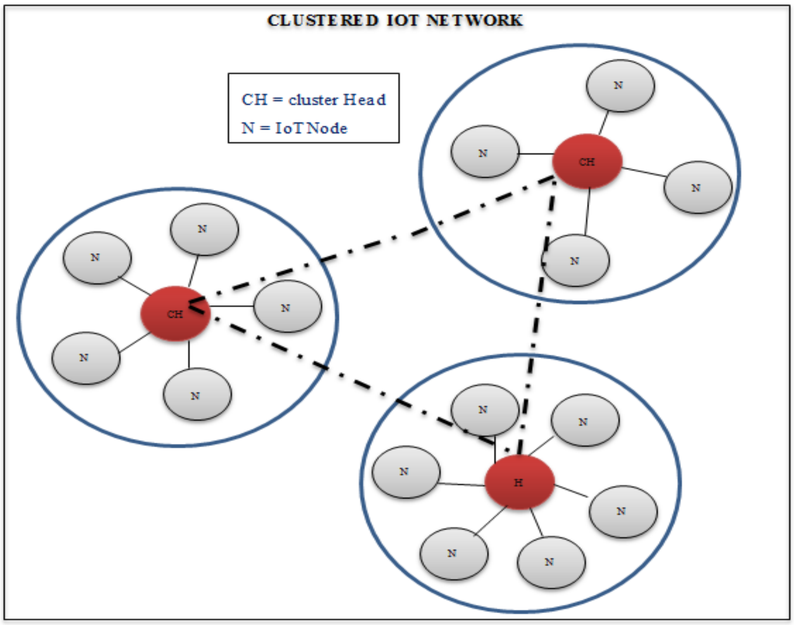

Fig..1 Clustering in WSN

3.2 Trust Evaluation

In this paper, a new multi-dimensional trust evaluation mechanism is proposed for IoT framework to detect the malicious nodes, which considers not only the social trust but also the Information trust. Meanwhile it reduces the possibility of misleading by malicious nodes in the process of trust evaluation through network related issues such as number of communication instances and the probability of successful data delivery. Also the trust evaluation responsibility is allotted to only the cluster heads with sufficient resources; thus the lifetime of network is prolonged.

3.2.1 Social trust

The social trust evaluates the trustworthiness of neighbour nodes by overhearing their transmission in promiscuous mode and dynamically identifies misbehaving nodes. Here the social trust is evaluated by the number of successful and unsuccessful transitions between the cluster head and the node. The cluster head overhears the node if it does not deliver a packet or transmits the packet in the predefined time interval. The acknowledgement about the success of packet delivery can be notified to the cluster head. If the packet sent by a node reaches the cluster head or other node in its routing table within a predefined time interval, it can be considered as a successful transition. Otherwise it is considered as an unsuccessful transition. For example if a node is compromised of selective forwarding attack or black hole attack, partial packets or all packets form the node will not reach the next node or cluster head. The higher the ratio of the number of successful transitions to the number of all transitions, higher the trust value. Based on this ratio, the cluster head evaluates the trust worthiness of node. Here the social trust is evaluated in two ways, one is direct evaluation and other is indirect evaluation. In the case of direct evaluation, the cluster head evaluates the trustworthiness of nodes through the direct evaluation of number of successful transitions to the number of overall transitions, whereas in indirect trust evaluation, the trustworthiness of an IoT node is evaluated through the neighbouring nodes of that IoT node. A simple schematic representing the direct and recommended trust is shown in figure.2

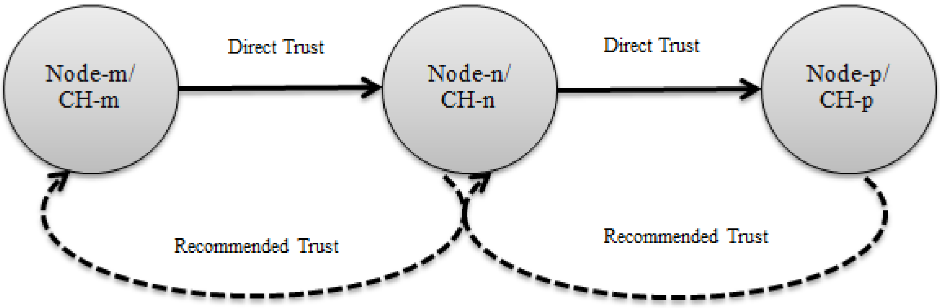

Fig.2 Schematic of Direct and recommended trust evaluation

The neighbouring nodes recommend the trustworthiness with regard to the cluster head. The social trust $ST_{CH,j}(t)$ can be defined as weighted aggregated sum of three components:

$$ST_{CH,j}(t) = w_1 DT_{CH,j}(t) + w_2 \frac{RT^{CH}_{k,j}(t)}{N_k} \qquad (1)$$

$DT_{CH,j}(t)$ denotes the degree of direct trust for CH for node *j* at time *t*, based on the node *i*'s observation of packet forwarding behavior for node *j*. $RT^{CH}_{k,j}$ is the indirect/recommended trust gained by the cluster head through the neighboring node *k* of node *j* at time *t*. N_k represents a set consisting of neighbors for node *j*. The weight factors w_1 and w_2 are assigned to $DT_{CH,j}(t)$ and $RT_{k,j}(t)$ respectively, such that $w_1 + w_2 = 1$, whereas $0 \leq w_1 \leq 1$ and $0 \leq w_2 \leq 1$. An indirect trust is determined from the observations gained through interactions with neighbours who notifies about their own direct observation for particular node. The indirect trust $RT_{k,j}(t)$ is determined using Eq. 2.

$$\sum_{k\in N_k, k\neq j} RT^{CH}_{k,j}(t) = \sum_{k\in N_k, k\neq j} DT_{CH,k}(t) \times DT_{k,j}(t) \qquad (2)$$

Where $DT_{CH,k}$ represents the direct trust between the cluster head CH and neighboring node *k* of node *j* and $DT_{k,j}$ represents the direct trust between the node *j* and neighbouring node *k*. Since there exists N_k number of neighboring node for every node, the summation is used as per equation (2). The evaluated indirect trust is exchanged as a part of recommendation with node *k*. Trust estimation involving trust degree of each node using indirect trust information brings several benefits. First of all, it speeds-up the convergence of trust evaluation process. Secondly, a node can detect and isolate misbehaving nodes at the earliest. Lastly, neighbours' recommendation information (indirect trust) enables the nodes that do not succeed in observing behaviour of their neighbours due to resource limitations.

3.2.2 Information trust

Information trust is the trust evaluation based on observing the Information, which is information oriented trust evaluated by cluster head CH. Since the IoT is a data-centric network, here the proposed approach introduces the information trust and the observed information is more effective in various applications. An example of this is tampering attack which can be detectable by this information trust.

In this trust evaluation, Euclidean distance is used to measure the trustworthiness of nodes towards the cluster head with regard to information transmission. As per standard notations, the mean and standard deviations of information forwarded by *k* different nodes is represented as m_{ak} and s_{ak} respectively. To evaluate the effective coverage of k-th dimensional information covered by different IoT nodes, the mean value of the observing information range is in the range of $[m_{ak} - s_{ak}, m_{ak} + s_{ak}]$. In the case of dense deployment of nodes in the IoT network, the acquired information having almost similar characteristics and the information with deviating can be considered as a malicious information. Further the node which has that malicious information can be detected as a malicious node. Therefore the information trust can be calculated as

$$IT_{CH,j} = [\exp(-D_{CH,j})] \qquad (3)$$

where

$$D_{CH,j} = \sum_{k=1}^{d_m} \sqrt{\left(x_{ik} - x_{jk}\right)^2} \qquad (4)$$

where $D_{CH,j}$ represents the Euclidean distance between the multi-dimensional effective average calculated by CH and the multidimensional information observed by information *j*, d_m indicates the dimensions of observing information; x_{ik} and x_{jk} represent the effective average of the *k-th* dimension information stored in CH and the *k-th* dimensional information of node *j*, respectively.

3.3 Composite routing metric

Based on the above trust evaluations, a new routing metric is evaluated which defines the degree of trustworthiness of IoT nodes. The combined routing metric, Overall Trust (OT) is defined as the summation of Social trust and the Information trust, represented as

$$OT_{CH,j} = \alpha * ST_{CH,j}(t) + \beta * IT_{CH,j} \qquad (5)$$

where α and β are two arbitrary constants which determine the weightage of social trust and information trust respectively and has to satisfy $\alpha + \beta = 1, s.t.\ 0 \leq \alpha \leq 1, 0 \leq \beta \leq 1$. The higher the weight, the more importance is given to that sub trust of the overall trust and vice versa. In the case of higher α, the overall trust constitutes with social trust and in the case of higher β value, the information trust is more consistent to total trust.

4. Simulation results

In this section, the proposed trust-aware framework is simulated to observe the performance in the detection of malicious nodes in the IoT network. Based on the trust observed in two ways, i.e., social trust and information trust, the overall trust is evaluated and the node which has less overall trust is considered as malicious node and a notification is given for remaining nodes in the network. To simulate the proposed framework, an IoT network with P number of nodes is created with an area of M x N, where M is the length and N is the width of the network. The simulation parameters are listed in table.1.

Table.1 Simulation Parameters

Parameter	Value
Number of nodes	30,50,70,100
Area	1000*1000 m^2

Number of clusters	0-10
Mac	IEEE 802.11
Simulation Time	50 Sec
% Malicious behavior	0-50% of total nodes
Traffic Source	CBR
Packet size	512
Trust threshold	0.6

Initially a random network is created with N number of nodes and the nodes which are higher on resources are selected as cluster heads. Since the proposed approach tried to maintain a trade off between the security and resource utilization, only the nodes which are rich in resource availability are taken as cluster heads. A simple representation of a network with 30 nodes and its clustered version are depicted in figure.3 and figure.4 respectively.

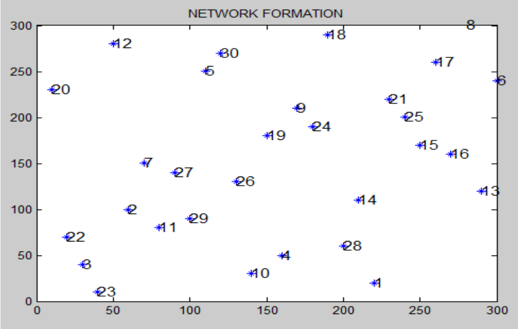

Fig.3 A random network

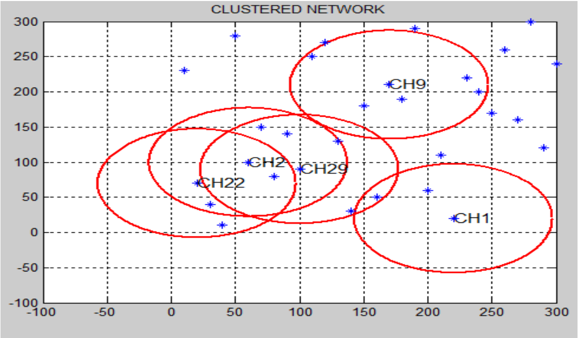

Fig.4 Clustered network

In the simulation study, the performance evaluation is carried out by measuring the performance metrics, Packet delivery ratio (PDR), packet loss ratio (PLR), Delay, Routing Overhead (RO) and Network Lifetime (NL) for varying number of malicious nodes. Since the proposed approach focused on the trust awareness, at every node the trust evaluation and the trustworthiness evaluation are accomplished with the surrounding neighbour nodes and based on the obtained trust values, one node is selected for further communication. This process is repeated at the cluster head level also if the destination is too far in which the multi-hop communication takes place. In the simulation study, the performance is evaluated by varying the % of malicious nodes as 5, 10, 15, 20 and 25. For example, if P = 30 nodes are there in the network, only 2 nodes are considered as malicious at 5% maliciousness. In this manner, the maliciousness of IoT network is increased and at every stage, the performance is measured based on the performance metrics through the proposed and conventional approaches. The obtained results are depicted in the following figures.

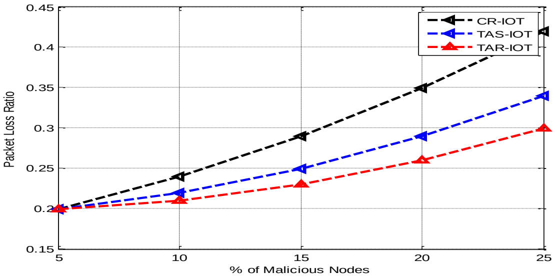

Fig..5 Packet loss ratio for varying malicious behaviour

As shown in figure.5, when the proposed approach is implemented over the Network, the PLR is observed as increasing in nature with increase in the number of malicious nodes. As the % of malicious behaviour increases, the number of malicious nodes also increases. This makes the network to compromise more and forces the adversary nodes to drop the packets instead of forwarding them. However, the PLR of proposed approach is less compared to the conventional approaches. Since the proposed approach accomplishes the trust evaluation with respect to both the social interactions and information acquired at every node. The packets transmitted from source to destination will reach more effectively and only few packets will be lost, whereas in the CR-IOT and TAS-IOT, the security evaluation mechanism didn't considered the multi-dimensional trust (ST and IT) which effects the packets transmission and forces the nodes to drop the packets.

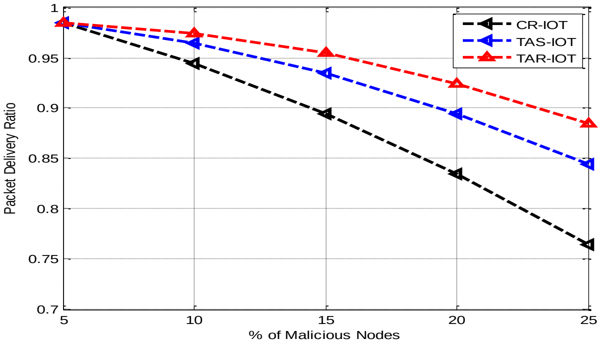

Fig.6 Packet Delivery ratio for varying malicious behaviour

When the maliciousness increases in the network, the attacked/compromised node won't help the other nodes in data transmission. Also, they try to drop the packets intentionally. When the packets are dropped at intermediate node due to their maliciousness, the packets won't reach the destination by which the packet delivery ratio decreases. This PDR will reach to lower levels with an increase in the malicious nature. It can be seen from figure.6 that the PDR is decreasing with increment the in the % of malicious nodes. However the PDR of proposed is observed to be high when compared to the conventional approaches. Due to the non-consideration of information trust in CR-IOT, the overall trust is just related to the social trust which reveals only the number of interactions. This process is not able to find the malicious nodes which are compromised through the data processing through them. Hence the conventional approaches can't provide sufficient PDR.

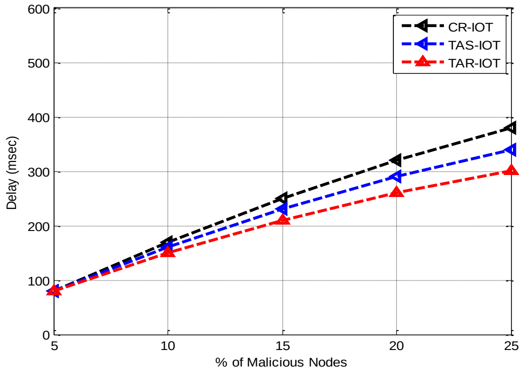

Fig.7 Delay (msec) for varying malicious behaviour

Delay is one more important metric which concerns the performance of a trust based security methods in the IoT. As the number of malicious nodes increase, the delay also increase, because, the malicious node won't send any notification about the packet forwarding or packet reception to the pre-hop node. The pre-hop nodes wait for TTL and reroutes the packet if it has not received any update from it's previous hop time. This rerouting process results in an increased delay. As it can be seen from figure.7, the delay of proposed approach is less even though there is an increase in the % of malicious nodes, because of the accomplishment of multidimensional trust evaluation in the selection of next hop node.

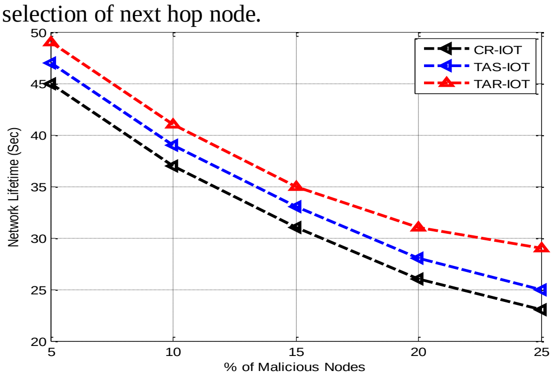

Fig.8 Network lifetime (Sec) for varying malicious behaviour

The smart and resource constraint natured devices used in the IoT based applications need be utilized in an organized way such that the overall network lifetime increases. The network lifetime is directly related to the energy being consumed at every node. As the malicious nature increases in the network, the reliable nodes need to search for route establishment again and again which results in an excessive power consumption. As the nodes loose energy, they will die and hence the overall network lifetime is also affected. As it can be seen from figure.8, the Network Lifetime is decreasing with increasing the number of malicious nodes. But, it is observed to be high when the network lifetime of conventional approaches is compared with proposed approach. Since the proposed routing methodology is effective in the selection of most trustworthy node, the information reached at that node won't get lost and the extra burden that occurs due to the rerouting will be avoided.

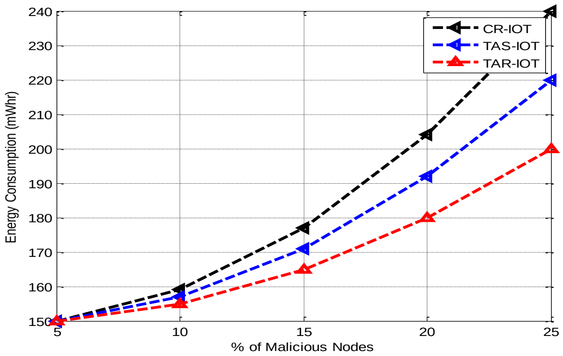

Fig.9 Average Energy Consumption for varying malicious behavior

As the number of packets increases, the amount of energy required to transmit those packets also increases. Hence the energy consumed is linearly related to the packet size. Here in the IoT based communication between the nodes, energy is a main resource constraint which needs to be preserved by designing an effective routing protocol. In this paper we have also focused to design an energy efficient routing protocol by clustering the network. The nodes which are richer in the resource (mainly energy) are selected as Cluster Heads and maximum communication process happens through them only. The nodes are chosen for helping only in the case of larger distances between the node and their respective cluster head. Further the malicious nature also affects the energy consumption of node. As the malicious nature increases, the nodes are subjected to rerouting in which the maximum power is required to throw the route request packet. If the security strategy is effective, then there is no need of rerouting which was the main drawback in the conventional approaches. Hence, it can be seen from figure.9, that the average energy consumption of proposed approach is less even though the malicious nature is increased.

5. Conclusion

Security is a critical aspect in the IoT based communications due to the vast heterogeneity of devices used in the network. In order to ensure the security in such type of communications, we need to consider the detection of malicious nodes which try to compromise the network in different ways. Keeping this in mind, a new secure and energy efficient framework is developed in this paper based on the social interaction occurring between the nodes and the information passing through them. Based on the earlier interactions and data, the trustworthiness of a node is decided here and if any node is found to be malicious, a notification is given to entire network indicating that particular node is malicious and other node should not communicate with it. Further to achieve an increased network lifetime and less average energy consumption, this framework followed the clustered strategy and most of the communication responsibility is allocated to the cluster heads. Simulation experiments are conducted over the proposed method with varying malicious rate and the performance is measured through the packet loss ratio, packet delivery ratio, delay, network lifetime and average energy consumption. The obtained results proved that the proposed approach is effective in securing the IoT system.

References

[1] L.A. Grieco, M.B. Alaya, T. Monteil, K.K. Drira, Architectinginformation centric ETSI-M2M systems, in: IEEE PerCom, 2014.

[2] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, Lithe:Lightweight Secure CoAP for the Internet of Things, IEEE Sensors Journal 13 (10) (2013) 3711-3720.

[3] H. Feng, W. Fu, Study of recent development about privacy andsecurity of the internet of things, in: 2010 International Conferenceon Web Information Systems and Mining (WISM), Sanya, 2010, pp.91–95.

[4] R. Roman, J. Zhou, J. Lopez, On the features and challenges ofsecurity and privacy in distributed internet of things, Comput.Networks 57 (10) (2013) 2266–2279.

[5] J. Anderson, L. Rainie, The Internet of Things will Thrive by 2025,PewResearch Internet Project, May 2014.

[6] G. Glissa, A. Rachedi, and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," in *2016 IEEE GlobalCommunications Conference (GLOBECOM)*, 2016, pp. 1-7.

[7] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "New trust metric for the RPL routing protocol," in *2017 8th InternationalConference on Information and Communication Systems (ICICS)*, 2017, pp. 328-335.

[8] T. Matsunaga, K. Toyoda, and I. Sasase, "Low false alarm rate RPL network monitoring system by considering timing inconstancybetween the rank measurements," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, 2014,pp. 427-431.

[9] C. Taylor and T. Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacksin smart grid networks," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, 2015, pp. 1835-1840.

[10] M. Surendar and A. Umamakeswari, "InDReS: An Intrusion Detection and response system for Internet of Things with6LoWPAN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*,2016, pp. 1903-1908.

[11] A. Le, J. Loo, K. K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology,"*Information*, vol. 7, p. 25, 2016.

[12] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in internet of things," *International Journal ofComputer Applications*, vol. 121, 2015.

[13] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and ComputerApplications*, vol. 42, pp. 120-134, 2014.

[14]J.Guo, I.-R. Chen, and J. J. P. Tsai, "Asurveyof trust computationmodels for service management in internet of things systems,"*Computer Communications*, vol. 97, pp. 1–14, 2017.

[15] J.-H. Lee and H. Kim, "Security and privacy challenges inthe internet of things [security and privacy matters]," *IEEEConsumer Electronics Magazine*, vol. 6, no. 3, pp. 134–136, 2017.

[16] C. V. L. Mendoza and J. H. Kleinschmidt, "Mitigating on-offattacks in the internet of things using a distributed trust managementscheme," *International Journal of Distributed SensorNetworks*, vol. 2015, Article ID 859731, 2015.

[17] H. Hellaoui, A. Bouabdallah, and M. Koudil, "TAS-IoT: Trust-Based Adaptive Security in the IoT," in *Proceedings of the 41stIEEE Conference on Local Computer Networks (LCN '16)*, pp.599–602, November 2016.

[18] O. Ben Abderrahim, M. H. Elhdhili, and L. Saidane, "TMCoISIOT:A trust management system based on communities ofinterest for the social internet of things," in *Proceedings of the13th IEEE International Wireless Communications and MobileComputing Conference (IWCMC '17)*, pp. 747–752, June 2017.

[19] F. Boustanifar and Z. Movahedi, "A trust-based offloading formobile M2M communications," in *Proceedings of the Intl IEEEConferences on Ubiquitous Intelligence & Computing, Advancedand Trusted Computing, Scalable Computing and Communications,Cloud and Big Data Computing, Internet of People,and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld '16)*, pp. 1139–1143, IEEE, 2016.

[20] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthysensing for internet of things in smart cities," *IEEE InternetofThings Journal*, vol. PP, no. 99, pp. 1-1, 2017.

[21] Y. Yu, Z. Jia, W. Tao, B. Xue, and C. Lee, "An efficient trustevaluation scheme for node behavior detection in the internetof things,"*Wireless Personal Communications*, vol. 93, no. 2, pp.571–587, 2017.

[22] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method forclustered wireless sensor networks based on cloud model,"*Wireless Networks*, pp. 1–21, 2016.

[23] Awais Ansari, GouriPatil, "A Novel Composite Routing Strategy to Enhance Trust and Network Lifetime in WSNs", IJATIR, June 2017.