ON THE ADVERSARY IDENTIFICATION IN WSN THROUGH LOCATION AND TRUST AWARENESS

Gouri R Patil
Associate Professor, MJCET, Hyderabad, India

Abstract: *Mostly all the sensors in Wireless Sensor Networks (WSNs) are deployed in resource constrained environment which leads a security threat to WSN. The provision of high-security becomes one of the challenges in wireless sensor networks. This paper proposes a new strategy called as Location and Trust Aware Routing (LTAR) in WSNs to provide the security in WSNs. LTAR introduces a new metric by combining two awareness's; they are Trust awareness and Location awareness. Trust awareness is evaluated based on the communication behavior of sensor nodes and it helps in the accurate identification of malicious whereas the location awareness is measured based on the rate of link connectivity through which the misclassification is reduced. Extensive simulations are carried out to validate the proposed LTAR. The performance of proposed method is evaluated based on malicious detection rate (MDR) and Throughput and it shows better results than the earlier approaches.*

Keywords: Wireless Sensor Networks, Malicious, Trust Awareness, Location Awareness, Rate of link Connectivity, and Packet Forwarding.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have attracted interest in a variety of applications, including, environmental monitoring, forest fire warning, , battlefield surveillance, intelligent home systems and health monitoring due to significant advances in sensor technology [1]. WSNs have become more important in various applications due to their unique qualities such as quick deployment, self-organization, and low cost. Sensor devices are the most basic components of a Wireless Sensor Networks, and they are quite inexpensive. As a result, the deployment cost of a WSN is significantly lower than that of a wired network. Furthermore, the sensors have self-organization characteristics, making the WSN resistant to a variety of conditions. The sensor nodes in the WSN will work together to provide communication support, allowing for a variety of high-level applications.

WSNs, on the other hand, are vulnerable to a variety of attacks due to the directness of the environment where the sensors deployed and the transmission medium. Furthermore, in multi-hop routing to forward the information to the base station, the sensor nodes seek the assistance of neighbor nodes in WSN. Due to the dispersed, open, and dynamic properties of WSN [2], [3], this multi-hop routing is subject to numerous attacks, posing a severe threat to information and data security. The algorithms which are developed earlier are now only defined for certain attacks. These attacks address specific malicious behavior or particular selfish behavior. So, they rely on authentication or encryption mechanisms that are not suited for multi-hop distributed and energy restricted WSN [4].

The proof provided by the present research work gives the effective output of Trust Management (TM) [5], [6] to provide the security WSNs. the traditional approaches are facing few problems to provide the security for Multi-hop networks. Currently, they are hands only few attacks but they are in lag to give the solution for new attacks. Further, the traditional approaches concentrating only on the achievement of an effective trust strategy but not concentrated on the constraints of resources and these approaches are not suitable for different environments like diverse topologies, diverse protocols etc.

This paper proposes a new routing mechanism called as Location and Trust Aware routing that considers the trust as well as location information to ensure a secure and Qualitative data transmission in WSNs. The proposed method introduced a new routing metric based on location information and packet forwarding behavior of nodes. For a given source and destination nodes, the final path is chosen based on the path trust which is an accumulation of lint trust between nodes.

Rest of the article is summarized as follows; Section 2 discusses the details of literature survey. Section discusses the details of proposed LTAR. The details of experimental analysis are explored in section IV and section V concludes the paper.

II. LITERATURE SURVEY

Recently, so many trust management techniques are introduced to implement Ad Hoc sensor networks. In [7], the authors proposed an ambient trust sensor routing (ATSR) to know the nature of misbehaving nodes in a network. In this work, few beacon messages are periodically broadcasted by each sensor node to know the

information about the location and the remaining energy levels. Further, each sensor node in the network multi-cast reputation request messages periodically to know the trust information indirectly. Moreover, this work consumes much energy in the network to broadcast and multicast of beacon messages. In [8], J. Duan et.al proposed trust aware secure routing framework (TSRF). In this work, each sensor node in the network get the information of indirect and direct trusts. Furthermore, an irregularity verification strategy has been integrated into this system to eliminate incorrect requests from malevolent or fraudulent nodes. The TSRF, on the other hand, does not store energy information, which means that the node chosen for data transmission could be drained before the data transmission is completed. Finally, this work does not provide the trust information fastly and consumes more energy.

In [9], the authors proposed Trust based "Friendship based Adhoc On demand Distance vector (AODV)" to defend black hole attack. In this work, Trust of each node is calculated based on identity of a node and its reputation [12] and at the same time assignment of attribute is done for each node. The sender node examines the attribute number by forwarding HELLO messages. When the hit occurs then the neighbor node get the permission to send the data packets to next node. But continuous HELLO packets transmission in the network requires more energy and they produce high traffic overhead. In [10], G. Zhan et al. proposed "Trust Aware Routing Framework (TARF)" to counter attack the black hole attack. In this work, the energy levels and trust information of each node is stored in their routing table. Here, the evaluation of trust is done based on the routing information of nodes through which malevolent nodes are get penalized. The major disadvantage of this technique is updation of energy levels of each node in the network are broadcasted by the control messages. This work suffers from Selfishness attack through which the wrong information may conveyed by the selfish node.

In [11], the authors proposed "Light Weight Trust based Routing protocol (LTB-AODV)" to defend black hole and gray hole attacks. To estimate the trust, this work uses Intrusion Detection System (IDS) which takes the help of each node's Packet Forwarding Behavior (PFB). Further, the authors not concentrated on each nodes energy constraints through which the death nodes probability gets increased and there may be the additive burden on trusted nodes. In [13], G. Han et al. proposed "an attack resistant model (ARTMM) for Under Water Acoustic Sensor Networks (UASNs)" by considering the multi-dimensional trust metrics. Node trust, link trust, and data trust are the three trust metrics through which calculation of trust is done in underwater environment. The trust calculation becomes complex when there is an unreliable communication and mobility. Due to this, this work is not suitable for all types of attacks.

In [14], the authors proposed a new trust mechanism for WSN called as "Light Weight and Dependable Trust System (LDTS)" to improve the reliability and to reduce the energy consumption of the network. Here, the clustering approach is used to reduce the energy consumption of the network. This work measures the light weight trust through total number of unsuccessful and successful interactions. Hence, this work not concentrated much on evaluation of residual energy through which the node will get the notification of network sustainability. In [15], K. Gerrigagoitia et al. proposed a new Intrusion Detection System through which intrusion is detected in WSNs. Here, the authors gave prime importance to the reputation of a node. This work evaluates the trust based on the beat function which includes incorrect and correct interactions between the nodes. The network overhead may increases because of intrusion detection and evaluation of trust of each node.

Hui Xia et al. [16] proposed a dynamic trust prediction model to assess the trustworthiness of mobile nodes in MANETs. This approach considered the historical behaviors and also the future behaviors via fuzzy logic rules prediction. This trust model is integrated with source routing mechanism. Further the route trust is measured as the product of intermediate nodes individual trusts. However, this approach considered only direct trust but not recommended trust which is most important since only the direct observations may mislead and results compromise. G. Dhananjayan and J. Subbiah [17] proposed a Trust Aware AdHoc routing (T2AR) to provide security in MANETs. T2AR method modified the conventional Adhoc On-demand Distance Vector (AODV) with the constraints of mobility, energy and trust rate for malicious node prediction. This approach employed both direct and indirect trusts and employed the matching between packet sequence ID and log reports of neighbor nodes to prevent the generation of malicious reports and also to improvise the security. Furthermore, they employed the Received Signal Strength indicator (RSSI) for the determination of trusted node where they are in the communication range or not. Muhammad Saleem Khan et al. [18] employed a Fine Grained Analysis (FGA) over packet loss to determine the real cause of packet loss and to discover the original malicious nodes. FGA measures the probability of packet forwarding based on MAC layer information, Queue Overflow and Mobility. Depends on the obtained probability, the sender node decides whether the node is malicious or not and the real cause of packet loss.

Deviating from the above methodology, Gouri Patil and Damodaram [19, 20] analyzed the threats in the network based on the concept of attack graph theory. However, they didn't considered the original behavior of sensor nodes to analyze their trustworthiness.

III. PROPOSED METHOD

This model is formulated based on the trust awareness between neighboring nodes in WSN. Under this model, we consider two nodes, one is Trust Agent (TA) and another is Trust Victim (TV). Here TA is defined as a node who measures the trustworthiness, and the TV is defined as a node whose trustworthiness is being measured. For trust computation, the TA node considers the trustworthiness of TV in different modes. Under trust evaluation, we consider two different modes of trust: they are direct mode and indirect mode. Finally a total trust is computed by combining these two modes of trust. Moreover, we modeled the trust evaluation with respect to location. Since the location is the main factor in WSNs, we have linked the trust evaluation with location. Based on these two modes of trusts, an overall trust of individual node is measured. For the computation of route trust, we consider the product of individual node's total trust.

3.1. Trust Computation

In WSNs, the trust is defined as a relationship between two neighbor modes. Here we define the trust model as a measure of integrity, timeliness and reliability of message to deliver to their next hop nodes. In this framework, we consider both node trust and route trust. Further the node trust is sub-categorized as Direct Node Trust (DNT) and Indirect Node Trust (INT). Here the node trust reveal the nodes quality of forwarding and the route trust reveals the quality of forwarding packets along the route. Irrespective of the trust models employed, they are broadly categorized as direct and indirect. The former one is in first-hand information which is obtained by the observation of TA on TV. However the second one is a trust obtained from indirect observations. Two types of trusts one measured here. They are;

Node interaction trust: this trust is calculated by the TV's one hop neighbor based on its behavior in the earlier communication interactions. Here we used two packet forwarding factors namely Data and Control. Further, to assess the importance of both factors, an individual weight is assigned to each factor. The overall trust of a TV is measured by combining these two factors.

Route Trust: This trust is calculated by the source node. For a given source and destination node pair, the source node computes route trust for available path's towards the destination node. This trust is employed to determine the quality of providing services along a route. When a source node decides to send data to destination node, it computes the credibility of the route. Route trust is assesses according to intermediate node's individual trust values over the route.

A. Direct Node Trust (DNT)

DNT is measured with respect to the packet forwarding behavior. Here the DNT is measured by TA based on the packet forwarding behavior of TV. Under this trust evaluation the TA node overhears their retransmission in promising mode and identifies the malicious nodes dynamically. Consider a node has become malicious; then it won't retransmit the packet to its further nodes. In such conditions, the sender node can't overhear the retransmission. Based on these behaviors, the TA measures the trustworthiness of TV node. Simply the DNT evaluation is expressed as an assessment of forwarding behavior of neighbor nodes by the sender node through the direct observation. Based on the observed behavior, the sender node assigns as trust value to its neighbor nodes after the transmission of packet sent by sender node to its neighbor node. Hence in DNT computation, we used the packet forwarding factor as a main reference parameter.

In WSNs, the entire packets are categorized in to two categories; they are control packets and data packets. Due to the possibility of both type of packets transmission in WSNs we have considered two packet forwarding factors namely control packet forwarding (CPF) factor and data packet forwarding (DPF) factor. After sending a packet the sender node waits for particular time to overhear the further retransmission. If it didn't overhear the further transmission, then it assumes the packet was dropped and sends another packet and overwrites the earlier send packet with recently sent packet. Consider two nodes x_a and x_b as truster and trustee respectively, the DNT, DNT(x_a, x_b) is measured as

$$DNT(n_a, n_b) = \alpha_1 \times CPF + \alpha_2 \times DPF \qquad (1)$$

Where CPF is the control packet forwarding factor, DPF is the data packet forwarding factor, α_1 and α_2 are the weights of CPF and DPF respectively. Here α_1 and α_2 are assigned in a such a manner they have to satisfy the condition $\alpha_1 > 0$ and $\alpha_2 > 0$ and $\alpha_1 + \alpha_2 = 1$. Next the CPF is measured as the ratio of total number of control packets forwarded correctly by node x_b to the total number of originally forwarded control packets by node x_a to node n_b. Similarly, the DPF is measured as the ratio of total number of data packets forwarded correctly by node x_b to the total number of originally forwarded data packets by node x_a to node x_b. Mathematically, the expression for CPF and DPF is expressed as

$$CPF \text{ or } DPF = \frac{C_p}{T_p} \qquad (2)$$

Where C_p is the totally number correctly forwarded packets and T_p is the total number of packets Forwarded actually. The both values C_p and $T_p$are the cumulative values from time 0 to *t*. Here correct forwarding means the forwarder node not only forwarding the packets to its next hop node but also forwarding correctly (no modification and if modification required then a correct modification). At this instant, there is a possibility to inert false information into the packets by forwarding nodes which makes the packet to reach to malicious parties of some other part of the network. For instance, if a malicious node forwards a packet after tampering with data, it is not considered as correct forwarding. If the sender notices this illegal notification, then the C_p value is decreased.

B. Indirect Node Trust (INT)

INT is provided by the common neighbour nodes of sender and receiver nodes. In INT, the TA seeks the opinions of common neighbor nodes to measure the trustworthiness of TV node. Simply we can understand that the common neighbor nodes have their own experiences about TV node and they share their opinions to TA node indirectly. The INT is measured with the help DNT between common neighbor node and TV node. For a given TA and TV nodes x_a and x_b the INT is computed as

$$INT(x_a, x_b) = DNT(x_a, x_k) \times DNT(x_k, x_b) \quad (3)$$

Where x_k is a common neighbor node for x_a and x_b, $DNT(x_a, x_k)$ is DNT between x_a and x_k and $DNT(x_k, x_b)$ is the DNT between x_k and x_b. Here the common neighbor node x_k shares its own experiences with x_a regarding the trustworthiness of trustee node x_b. The INT is a trust chain mechanism means it is exchanged as a part of communication with the node x_a. The recommended trust has several advantages; (1) Convergence time is very low and speeds of the process, (2) The source node identity and separates the malicious node earliest and (3) Recommended Trust enables the nodes that are not able to observe the behavior of its neighbor node due to resources constrains. Figure.1 shows the simple schematic representation Direct and Recommended trusts evaluation.

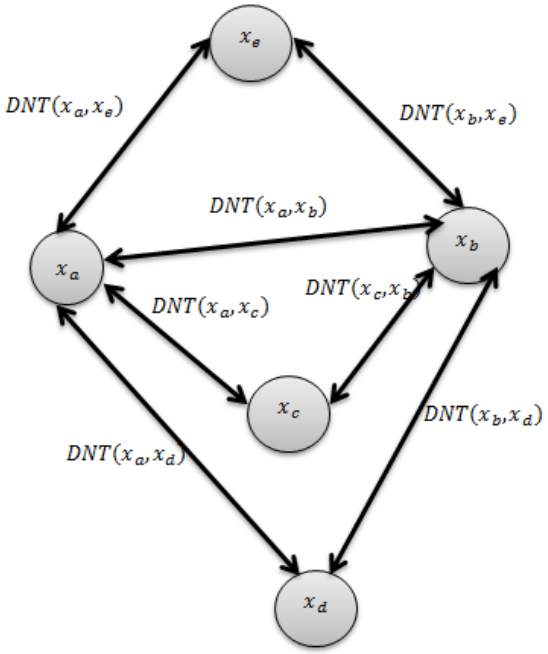


Figure.1 DNT and RNT Computation

C. Total Trust

The overall trust is measured by combining the Direct Trust and Recommended Trust. Mathematically the Total Trust is represented as;

$$OT(x_a, x_b) = DNT(x_a, b_b) + \frac{1}{B}\sum_{i \in Common\ nodes} INT_i(x_a, x_b) \quad (4)$$

Where B is the total number of common neighbor nodes for x_a and x_b. Since there exists more than one common neighbor nodes, the INT is obtained as an average of neighbor node's opinions. Hence we have applied the average formula at second term in Eq.(4). $INT_i(x_a, x_b)$ represents the INT between the nodes x_a and x_b and

it is recommended by the i_{th} common neighbor node of nodes x_a and x_b. For the example representation shown in Figure.1, the total trust is computed as follows;

$$OT(x_a, x_b) = DNT(x_a, b_b) + \frac{1}{3}\sum_{i \in Common\ nodes} INT_i(x_a, x_b) \quad (5)$$

$$OT(x_a, x_b) = DNT(x_a, b_b) + \frac{1}{3}\sum_{i=e,c,d}^{3} INT_i(x_a, x_b) \quad (6)$$

$$OT(x_a, x_b) = DNT(x_a, b_b) + \frac{1}{3}\begin{pmatrix} INT_e(x_a, x_b) + \\ INT_c(x_a, x_b) + \\ INT_d(x_a, x_b) \end{pmatrix}$$

(7)

$$OT(x_a, x_b) = DNT(x_a, b_b) + \frac{1}{3}\begin{pmatrix} \left(DNT(x_a, x_c) * DNT(x_c, x_b)\right) + \\ \left(DNT(x_a, x_e) * DNT(x_e, x_b)\right) + \\ \left(DNT(x_d, x_c) * DNT(x_d, x_b)\right) \end{pmatrix} \quad (8)$$

Note: At INT, there is a possibility of malicious nodes to send false reports. For example a malicious node may tamper with data and can miss guide to route the packet to other malicious node or forwards the packet to some other part of network. To avoid this problem, we e consider the correct packet forwarding results only. At the calculation of forwarding factors the packets those were correctly forwarded to intended node are only considered.

D. Location Awareness

Most of the existing methods have considered only packet forwarding behavior as a main reference for the trustworthy node selection. If the packet loss is observed at any node, it is simply considered as a malicious node and discarded from the network. However, the packet forwarding behavior may get affected due to so many problems. Moreover, the earlier methods neglected the impact of time periods of communication interactions. For example, the packet loss occurred in the previous time interval has high impact on the trust values than that is the earlier intervals. The main reason behind this issue is the location shifting of sensor nodes. Due to the shift in the location of nodes, they move away from the nodes which cause to lose the overhearing of nodes retransmission. For a sender node which sent the packet to its next hop nodes, it has to make sure to overhear the retransmission of that packet to the following hop in promiscuous mode. A successful overhearing only reveals the successful delivery of packet to intend destination. If the sender node overhears the packet forwarding from the next hop node, then only it is considered as successful interaction otherwise it is declared as malicious behavior. In some cases where the sender node cannot overhear the retransmission of its packet even though it was happened or a destination is unreachable due to stale routing information then the forwarding node is declared as malicious node. Due to this reason, location information is much important factor which needs to be considered during the trust computation. A node can evaluate the location variability of its neighbor node by computing the Rate of Link Connectivity (R_L) in the neighborhood. Such R_L can be used to analyze reasons of packet loss. The R_L at node x_a can be determined as

$$R_L(x_a) = A_L(x_a) + D_L(x_a) \quad (9)$$

Where $R_L(x_a)$ is rate of link connectivity at node x_a, $A_L(x_a)$ is the Arrival of Links and $D_L(x_a)$ is the departed links at node x_a. Consider $\max(A_L(x_a))$ is maximum A_L and $\max(D_L(x_a))$ is the maximum D_L, based on results shown in [88] the rate of R_L is formulated as

$$\max(A_L(x_a)) + \max(D_L(x_a)) = 2.\sigma(x_a) \quad (10)$$

Then the rate of R_L can be expressed as

$$\delta = \frac{A_L(x_a) + D_L(x_a)}{2.\sigma(x_a)} \quad (11)$$

Based on Eq.(11), the probability of successful packet forwarding with respect to rate of link changes is formulated as

$$P(x_a) = 1 - \delta \quad (12)$$

Based on Eq.(5.11) we can determine that the higher R_L indicate more dynamic nature and consequence to less probability of successful packet forwarding. Finally node x_a computes the node $x_b's$ trustworthiness according to the Rate of Link Connectivity, the overall trust is modified as

$$OT(x_a, x_b) = OT(x_a, x_b) * P(x_a) \quad (13)$$

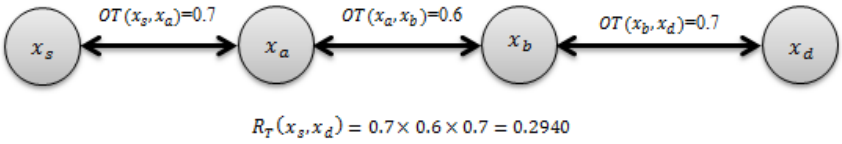
Here the final $OT(x_a, x_b)$ signifies the trustworthiness of node x_b with respect to its neighbor node's R_L. The main advantages with the involvement of location information in trust computation are to ensure an accurate identification of malicious nodes.

E. Route Trust Computation

The route trust is measured by combing the trust of intermediate nodes on every route. For a given source and destination node pair, the route trust is computed as

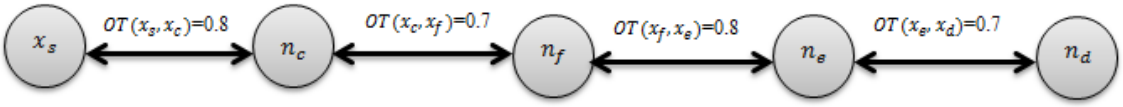
$$R_T(x_s, x_d) = \prod(OT(x_a, x_b) | x_a, x_b \in R, x_a \rightarrow x_b) \quad (14)$$

Where $x_s$is source node and x_d is the destination node of route R and $x_a \rightarrow x_b$ indicates that the node is x_a and x_b are neighbor nodes and they are directly connected to each other. Figure.2 shows a simple representation of route trust computation followed by route selection.



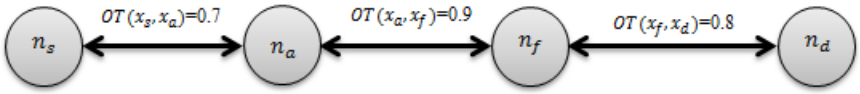
$R_T(x_s, x_d) = 0.7 \times 0.6 \times 0.7 = 0.2940$

(a)



$R_T(x_s, x_d) = 0.8 \times 0.7 \times 0.8 \times 0.7 = 0.3136$

(b)



$R_T(x_s, x_d) = 0.7 \times 0.9 \times 0.8 = 0.5040$

(c)

Figure.2 Route trust computation

As shown in the above figure, the first route (shown in Figure.2a) has the route trust of 0.2940, for the second route (shown in Figure.2b), the route trust is 0.3136 and the third route (shown in Figure.2c) have route trust is 0.5040. These values are obtained after the substitution of individual Total trusts into the Eq.(14). From these values, we can see that the maximum route trust is observed at third route. Hence it is selected as final route for data forwarding from source to destination.

IV. EXPERIMENTAL ANALYSIS

For the purpose of Experiments, we have considered different types of parameters and they are shown in Table.2. For the simulation experiments purpose, we created a random network with N number of mobile nodes. The area of deployed network is considered as $1000\text{ m} \times 1000\text{ m}$. Within this network area, we deployed different number of nodes like 30, 40 and 50. The communication range of each nod is considered as $1/4^{th}$ of network area, i.e., $\frac{1}{4} * 1000 = 250$ m. Means, every node can communicate with the nodes those are under the communication range of 250 m from itself. For mobility realization, we have employed random way point model. According to this model, the node speed is chosen in a random fashion and the node moves from one location to another location randomly. Similarly, to study the effect of malicious nodes, we have varied the % of malicious nodes from 0 to 40%. The traffic type is considered as constant bit rate and the size of each packet is considered as 512 bytes. The simulation time is considered as 200 seconds with the pause time of 5 seconds. The data rate of each link is assumed as 2048 bytes/sec.

Table.1 Simulation parameters

Network Parameter	Value

Number of nodes	30
Network Area	1000 m × 1000 m
Communication Range	250 m
Malicious nodes	10-40% of total nodes
Mobility Model	Random Way point
Simulation Time	200 Seconds
Pause time	5 Seconds
Packet size	512 bytes
Data rate	2048 bytes/sec
Trust Threshold	0.6

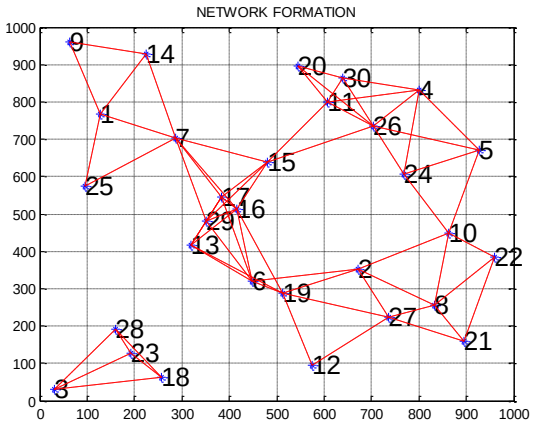


Figure.3: Network created with 30 nodes

For a given network as shown at Figure.3 with 30 nodes, node 21 is selected as source node and node 20 is chosen as destination node. For this source and destination node pair, there exist 10 possible paths. Among the available paths, Path 4 is chosen as optimized path because it has Higher Total trust and lower rate of link connectivity. The values of remaining un-optimized paths are shown in Table.2. The optimized path is highlighted with red color.

Table.2: Available paths and optimized path

No.	**Path**	*DNT*	*INT*	*OT*
Path 1	21→22→10→5→4→30→20	0.86	0.81	1.67
Path 2	21→8→10→24→26→20	0.91	0.85	1.76
Path 3	21→27→19→6→17→15→11→20	0.88	0.72	1.60
Path 4	**21→27→19→16→15→11→20**	**0.95**	**0.87**	**1.82**
Path 5	21→22→10→24→26→11→30→20	0.82	0.80	1.62
Path 6	21→8→10→5→4→30→20	0.81	0.55	1.36
Path 7	21→27→20→10→24→26→4→30→20	0.85	0.59	1.40
Path 8	21→8→27→2→19→6→29→15→11→20	0.87	0.76	1.62
Path 9	21→27→12→19→6→13→17→15→11→20	0.79	0.65	1.44
Path 10	21→22→8→10→24→4→11→20	0.83	0.75	1.58

For the comparison purpose, we referred most relevant and recent methods; they are Fine Grained Analysis (FGA) [18], Dynamic Trust Prediction Model (DTPM) [16], and Trust Aware AdHoc Routing (T2AR) [17]. Here, we evaluate the performance of LTAR by varying the malicious node count. The range of malicious nodes is varied from 0 to 40% of total nodes. When the value of malicious node count is 0, then it denotes the network is more secure. For 10%, the total number of malicious nodes present in the network is 10% of total nodes. For example, consider the total number of nodes in the network is 40, then 10% means $40 \times \frac{10}{100} = 4$ are malicious nodes. Similarly, for 20%, we will get eight, for 30% we will get 12 and for finally for 40%, we will get 16 malicious nodes.

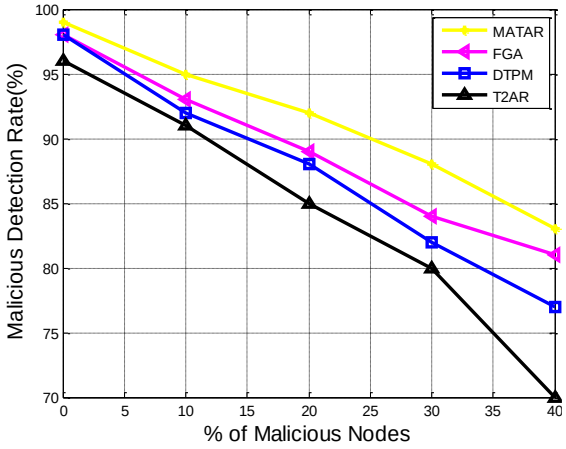


Figure.4 MDR for varying malicious nature

Figure.4 shows the comparison of MDR for varying malicious nature in the network. As the malicious node count increases in the network, the MDR decreases. It is a known fact that as the malicious nodes are more in network, they cause a serious damage to the network and the detection becomes harder. Since there are different types of attacks, each malicious node may be compromised by a different attack which makes the detection harder. From the Figure.4 we can see that the proposed LTAR has gained a better MDR at every instant of % of malicious nodes. Even though the T2AR employed direct and indirect observations for trust computation, there is no concept of correct packet forwarding concept. Hence the sender node can't take a correct decision regarding the malicious nature because even though the forwarding node tampered and forwarded that data, the sender node can't identify it, because the sender overhears the packet's further forwarding successfully. There is some kind of attacks which tamper the data and for such kind of attacks T2AR shows poor performance. Next, the method proposed in DTPM considers only direct observations and hence it has gained less MDR.

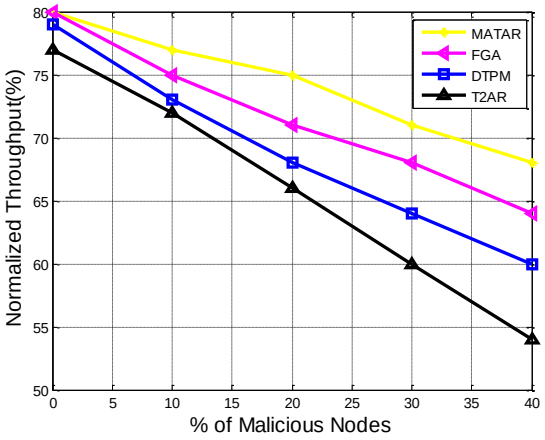


Figure.5 NT for varying malicious nature

Figure.5. reveals the details of QoS parameter i.e., Normalized Throughput comparison. With an increase in the malicious nature of network, the compromised/attacked node won't cooperate to other nodes for data transmission. Once the route is broken or misguided due to the malicious node, there is a need of an additional time required to establish the route or to forward the data again to intended nodes. This process consumes more time and results in less throughput since the throughout and time have inverse relation. Since the proposed LTAR employed location assisted trust assessment, the link breakages due to location change will get notified. This process lessens the time consumption thereby attains a higher throughput even at larger malicious node count. The method focused on FGA didn't consider the packet forwarding ratio of nodes and hence it has gained less throughput. Further DTPM didn't consider the indirect trust and hence the neighbor nodes with malicious nature drop the packet and pretend like a normal node. On an average, the Normalized Throughput of proposed approach is observed as 74.9866% while for existing methods, it is observed as 71.4478%, 68.9685% and 65.9963% for FGA, DTPM and T2AR respectively.

V. CONCLUSION

In this paper, we mainly concentrated on the provision of a secure and qualitative data exchange between sensor nodes in WSNs. Towards such prospect; we propose a new method based on the communication behavior and location shift of sensor nodes. For a given source and destination node pair, every node chooses a trustworthy and stable node as a next hop forwarder and establishes a secure path. At the assessment of communication behavior, we used packet forwarding nature of nodes and at location assessment, we used rate of link connectivity. The change in communication behavior ensures a correct identification of malicious nodes while the location awareness protects the innocent nodes. Simulation through varying malicious node count shows the effectiveness of proposed method.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102-114, Aug. 2002.
[2] E. Adel, K. Abdellatif, and E. Mohammed, ``A new trust model to secure routing protocols against DoS attacks in MANETs," in *Proc. 10th Int. Conf. Intell. Syst. Theories Appl. (SITA)*, Taipei, Taiwan, Oct. 2015, pp. 1-6.
[3] J.-M. Chang, T. Po-Chun,W. G. Isaac, C. C. Han, and C. F. Lai, ``Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Syst. J.*, vol. 9, no. 6, pp. 65-75, Jun. 2015.
[4] X. Du and H. H. Chen, ``Security in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 60_66, Aug. 2008.
[5] Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, ``ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 2013-2027, Sep. 2016.
[6] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, ``An accurate and precise malicious node exclusion mechanism for ad hoc networks," *Ad Hoc Netw.*, vol. 19, no. 6, pp. 142-155, 2014.
[7] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, “A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks,” *Wirel. Pers. Commun.*, vol. 69, no. 2, pp. 805–826, Apr. 2012.
[8] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, “TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks,” *Int. J. Distrib. Sens. Networks*, vol. 2014, no. Article ID 209436, pp. 1–14, 2014.
[9] T. Eissa, S. Abdul Razak, R. H. Khokhar, and N. Samian, “Trust-Based Routing Mechanism in MANET: Design and Implementation,” *Mob. Networks Appl.*, vol. 18, no. 5, pp. 666–677, Jun. 2013.
[10] G. Zhan, W. Shi, and J. Deng, “Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs,” *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 2, pp. 184–197, 2012.
[11] N. Marchang and R. Datta, “Light-weight trust-based routing protocol for mobile ad hoc networks,” *IET Inf. Secur.*, vol. 6, no. 2, pp. 77–83, 2012.
[12] S. Ganeriwal and M. Srivastava, “Reputation-based framework for high integrity sensor networks,” *ACM Trans. Sensor Netw.*, vol. 4, no. 4, pp. 66-77, Oct. 2004.
[13] G. Han, J. Jiang, L. Shu, and M. Guizani, ``An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447-2459, Dec. 2015.
[14] X. Li, F. Zhou, and J. Du, ``LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924-935, Jun. 2013.
[15] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, and I. Arenaza, ``Reputation-based intrusion detection system for wireless sensor networks," in *Proc. IEEE Complex. Eng.*, Jun. 2012, pp. 1-5.
[16] Hui Xia, Zhiping Jia, Xin Li a, Lei Ju, Edwin H. M. Sha, “Trust prediction and trust-based source routing in mobile ad hoc networks”, Ad Hoc Networks 11 (2013) 2096–2114.
[17] G. Dhananjayan and J. Subbiah, “T2AR: trust-aware ad-hoc routing protocol for MANET”, *SpringerPlus (2016) 5:995.*
[18] Muhammad Saleem Khan, Daniele Midi, Majid Iqbal Khan, and Elisa Bertino, “Fine-Grained Analysis of Packet Loss in MANETs”, *IEEE Access*, Volume 5, 2017, pp. 7798-7807.
[19] Gouri R Patil, A. Damodaram, “A Short-Normalized Attack Graph Based Approach for Network Attack Analysis”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, Volume 16, Issue 3, Ver. IX (May-Jun. 2014), PP 06-12.
[20] Gouri R Patil, A. Damodaram, “Quality Restrain Coding in Network Security Using Optimal Attack Graph Modeling”, IJAER, Vol.10, pp. 0973-4562.