



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Evaluation of Improved Trust Architecture (ITA) for Wireless Sensor Networks

B.A.Sabarish (Asst.Prof)^[1], M.Priyanka^[2], G.Agalya^[3], Sarayu.S^[4]

Department of Information Technology, Amrita School of Engineering, Ettimadai

Abstract: *Wireless Sensor Networks has been applied in various levels of applications in the real world. Applications are requires correct and error free information for decision making process. The sensor nodes are distributed across the open air environment where security is important issue. The information communicated among the nodes should be secure from threats like Sinkhole attack, Wormhole attack, etc. Trust plays a major role in data management which provides better decision making. The information must be collected from the trusted nodes of the network. The existing trust architectures calculate the trust based on the acknowledgement and broadcast messages from the nodes. An improved architecture discussed in this paper, Improved Trust Architecture (ITA), considers a three level architecture to provide better trust in the networks. It considers various factors such as Rate of Packet Reception (PRR), Rate of Packet Sent (RPS), Transmission Rate (TR), Data Consistency Rate (DCT), and Node Availability (NAV). The levels are organized with reference to the OSI Layers of a network.*

Keywords: WSN, ITA, TARF, Probabilistic Acknowledgement

I. Introduction

The Wireless Sensor Networks (WSN) is a collection of distributed sensor nodes to work together for monitoring the physical, environmental conditions and track the moving objects like vehicles, animals and predict their behaviour. It is also used in many real time applications such as military applications, battlefield, air quality monitoring network infrastructure, forest fire detection [9], etc. WSN comprises of sensor nodes with limited communicating capabilities, less computation power, deployed in the environment to detect the events and report back to the cluster head or base station. The nodes transmit the data through the open air medium to the base station which is open to attacks like fail-silent or byzantine failures. These failures motivate to create a new framework to ensure the security and reliability of the network to identify and detach the malfunctioning nodes from network. Trust of the nodes create security and ensures that the right data is received at the base station. Due to the wireless nature of the nodes, there are possibilities of various attacks. So, the trust framework that addresses the security, reliability, privacy, robust, authentication and authorization in the wireless sensor networks is very important. But security is still a fundamental and composite bottleneck in WSN. In order to overcome this problem, a trust management system for sensor nodes is required. In WSN, trust is the combined characteristics model for providing security, reliability, privacy with respect to the mobility[3], [4], [5], [10]. It is the level or the degree of confidence that a node can have on another node. A trust management system is useful for detecting a node which is not behaving as expected (either faulty or maliciously) or it can assist in the decision-making process [11].

Many existing trust management system in WSNs are mainly based on the acknowledgement given by the nodes and broadcast messages from the base station [2]. Many drawbacks are encountered while receiving acknowledgement from the nodes such as time delay, two army problem, and heavy traffic in the network. This may lead to fault rejection of the nodes. To reduce the fault rejection, ITA [1] includes various factors to calculate the trust of the nodes. ITA has also overcome sinkhole attack, wormhole attack, sybil attack, and network hole attack. This paper mainly concentrates on the evaluation of nodes based on the trust factors and calculation of aplomb level and detect whether the node in the sensor network is a malicious or trusted node. If the node is identified as a malicious node then that particular node will be detached from the network to increase security and reliability of the network.

II. Motivation

Wireless sensor networks uses multi-hop routing for the transmission of information from the node to the sink point and base station. Multi-hop suffers heavy traffic due to acknowledgement and broadcasting. Attackers may send invalid number of transmissions to flood the network and create collision which results in information loss. Available trust management focuses on the broadcast messages sent from the base station which may be lost due to traffic created by flooding or network jamming. ITA considers various trust factors in three levels to calculate the trust and reduce the fault rejection of honest node in the network [1]. The trust factors includes Rate of packet reception which is used to find the amount of packet that has been received, Rate of packet sent which helps to find number of packets sent from one node to another, Data consistency rate is the expected time by which the packets should be delivered to the receiver, Transmission rate is the number of packets transmitted from one node

to another in the transmission channel, Node availability is used to find whether the neighbouring node is available or not [7], [8]. When the node satisfies these conditions then the node is said to be trusted otherwise it is a malicious node. ITA implements these trust factors in order to calculate the trust of the node and compares it with the threshold value to identify the trusted and malicious nodes. Malicious nodes are then detached from the network. ITA is implemented in three levels as shown in figure 1.

NAV				Level 3
DCT				Level 2
PRR	RPS	TR		Level 1

Figure 1: Architectural diagram for ITA

The layer is organized with reference to the OSI Layer of the networks. Layer 1 deal with physical layer of the network to check the reliability of the path. Layer 2 deals with the Data Consistency rate which lies in the network and transport layer to monitor communication behaviour of the node in the network. Layer 3 deals with session layer to check the availability of the node for the communication at that point of time.

III. Related Work

A. Design

ITA secures WSNs against intruder by evaluating the aplomb level which is the measure of trustworthiness of the node. Considered a hybrid topology to implement trust is given in the figure 2. The topology consists of five clusters, each consisting of 100 nodes, summing to 500 nodes. These clusters contain many sub clusters with different topologies range from star topology to hybrid topology. Each cluster maintains a different topology and they will be regrouped to new clusters, when they move from one location to other. ITA has been tested on all the topologies to ensure it works efficiently.

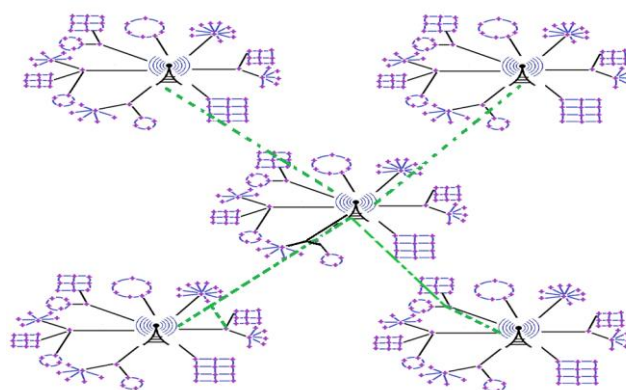


Figure.1

B. Implementaion

In order to evaluate and ensure the security provided by ITA, NS2 simulation is used. In the experiment, initially 500 nodes are distributed in the network with unreliable wireless transmission. All the nodes are assigned with different power level and moving patterns. The nodes in the sub clusters transmit the packets to their respective heads through single hop or multi hop routing. In turn, these head nodes transmit the packets to the base station provided for each clusters. The Traffic information retrieved from the trace files generated by NS2act as the input for calculating the trust factors of ITA. The calculation of the trust factors and identifying the trustworthiness of the nodes are implemented using AWK files and OTcl & C++.

In ITA, the trust factors are evaluated to calculate the aplomb level. The level 1 in the ITA architecture comprises of three factors Rate of packet reception (PRR or prr), Rate of packet sent (RPS or rps) and Transmission rate (TR or tr). The amount of packet that has been received by the node during the transmission is rate of packet reception (PRR). The received packet by the node at time t and $(t-1)$ are used as the inputs to calculate PRR. The PRR value can be calculated using the formula,

$$PRR_{(a,b)}(t) = \frac{PR_{(a,b)}(t) - PR_{(a,b)}(t-1)}{PR_{(a,b)}(t) + PR_{(a,b)}(t-1)}$$

where $PR(t)$ is the packet reception at time t and $PR(t-1)$ is the packet reception at time $t-1$. If the calculated PRR satisfies the minimum required threshold value then it is accepted. The rate of packet sent RPS is used to find the

amount of packet that has been sent when there exists communication between the nodes. The inputs to calculate RPS are the actual number of packets required and the number of repeated packets during the transmission. The formula for finding the rate of packet sent is given by,

$$RPS_{(a,b)}(t) = \frac{ANP_{(a,b)}(t)}{ANP_{(a,b)}(t) + RP_{(a,b)}(t)}$$

where ANP is the actual number of packets required and RP gives the packets that should be repeated. Using this information RPS is calculated. If the calculated RPS is above the threshold then the factor is accepted.

The last factor in the level 1 is Transmission rate (TR). But before calculating TR the aplomb level is identified for the node. If both PRR and RPS fail to satisfy minimum threshold value then level 1 fails, so there arises no need to calculate TR and the status of the node is marked as malicious. If any one of the factors, PRR or RPS, satisfies the condition then aplomb level of the node is updated and TR is calculated. The required Boolean condition to proceed to the calculation of next factor TR is

$$(pr \parallel rps) = 1 \ \&\& \ (pr \&\& rps)! = 1$$

The rate at which data flows from one node to another during routing is identified by the transmission rate. The number of packets transmitted from one node to other node at time t and $(t-1)$ are the inputs to evaluate TR. $TR_{a,b}(t)$ is calculated using the formula,

$$TR_{(a,b)}(t) = \frac{TP_{(a,b)}(t) - TP_{(a,b)}(t-1)}{TP_{(a,b)}(t) + TP_{(a,b)}(t-1)}$$

where $TP_{a,b}(t)$ is the number of packets transmitted at time t and $TP_{a,b}(t-1)$ is the number of packets transmitted at time $(t-1)$. When TR satisfies the threshold value then it is accepted.

To satisfy the condition of level 1, either all three factors pr , rps and tr must be true or the factors must have any one of the values as mentioned in the table below:

pr	rps	tr	Trust Level
T	F	T	1
F	T	T	1
T	T	F	1

Table. 1.

When level 1 conditions are satisfied then the aplomb level of the respective node is updated or else the node is marked as malicious.

The factor present in level 2 is Data Consistency rate (DCT). The degree of difference in sending data packets between the nodes is given by the data consistency rate. Based on the capacity of the node the number of consonant and dissonant packets varies. Using these as the inputs, the information is collected from the trace file and DCT is calculated. $DCT_{a,b}(t)$ can be calculated using the formula

$$DCT_{(a,b)}(t) = \frac{CS_{(a,b)}(t)}{CS_{(a,b)}(t) + DS_{(a,b)}(t)}$$

where $CS_{a,b}(t)$ is the number of consonant packets and $DS_{a,b}(t)$ is the number of dissonant packets. If the value of DCT is above the threshold, then the level 2 condition is satisfied and aplomb level is updated. The new aplomb level specifies that the level 1 and level 2 are satisfied for a node. The final level in the ITA architecture is level 3 which consists of Node availability (NAV) factor. To know the presence of the node in the network the factor NAV is used, which is based on probabilistic acknowledgement [6]. From the trace file, the broadcasting message with its acknowledgement is taken as the input to calculate NAV. $NAV_{a,b}(t)$ is calculated using the formula,

$$NAV_{(a,b)}(t) = \frac{ACK_{(a,b)}(t)}{ACK_{(a,b)}(t) + NACK_{(a,b)}(t)}$$

Where $ACK_{a,b}(t)$ is the number of packets that has been responded at time t and $NACK_{a,b}(t)$ is the number of packets that have not been responded at time t . If NAV is above the threshold value then level 3 is satisfied and aplomb level is updated. The status of the node can be identified using the aplomb level. The aplomb level for the node is satisfied when

$$[(\text{Level 1}) \&\& (\text{Level 2}) \&\& (\text{Level 3})] = 1$$

When the aplomb level for the node is satisfied with the minimum required value then the node is trusted else it is marked as a malicious node.

Using ITA, the malicious nodes in the network of 500 nodes are identified within 0.35-0.45 seconds. As soon as the node is found to be malicious it is detached from the entire network. In the experiment, nearly 245 links are detached in the network because of the identification of malicious nodes. If neighbours of the malicious nodes are trusted nodes then those neighbouring nodes search for a nearby trusted node to establish a new connection. So, the trusted nodes participate in the network even though their neighbour is malicious. This process will help in the inclusion of all the trusted nodes in the network which will increase the trustworthiness of the network. It improves security and reliability of network by reducing Fault Identification and rejection of nodes.

IV. Result

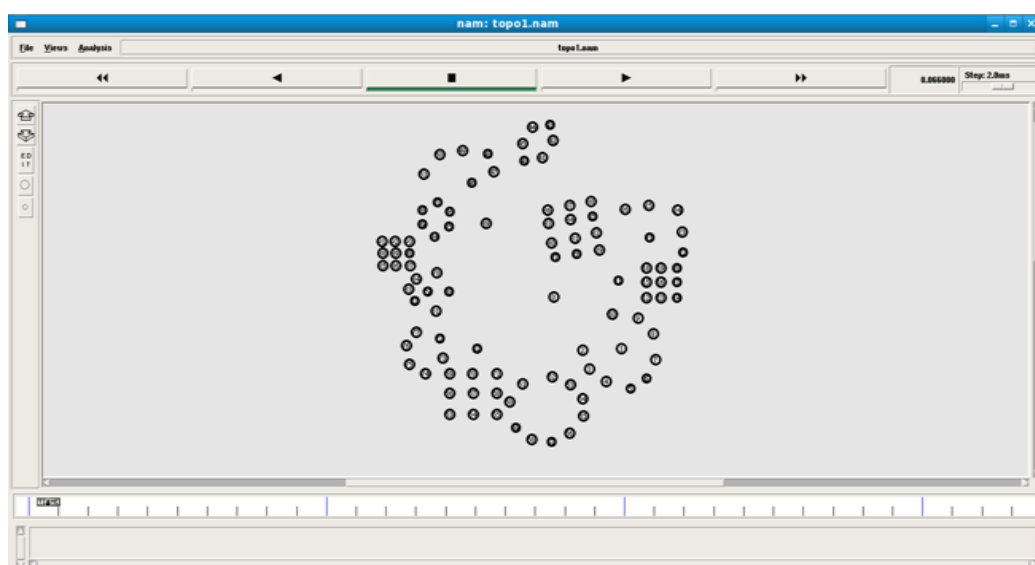


Figure 3: A snapshot of the simulated network

The above sub-cluster in figure 3 has 100 nodes, which is a part of the 500 node architecture. The sub clusters in the above cluster consists of mesh, star and ring structure. This combined architecture is considered so that the performance of ITA can be tested on all the topologies and proved to be efficient. The initial considerations of the nodes in the architecture are trusted and are eligible for the communication purpose. Each node communicates through a single hop or a multi hop path to reach the head node of each cluster. The clusters will be connected to each other via a node present on the other cluster.

By executing ITA, the malicious nodes are identified and marked with red as shown in figure 4. The nodes that are marked failed to satisfy the trust condition. The number of malicious nodes obtained is 29. The communication link of these nodes with the other nodes in the cluster will be detached. The other trusted nodes that are present in the network will connect to the next nearest trusted node and continue the communication process

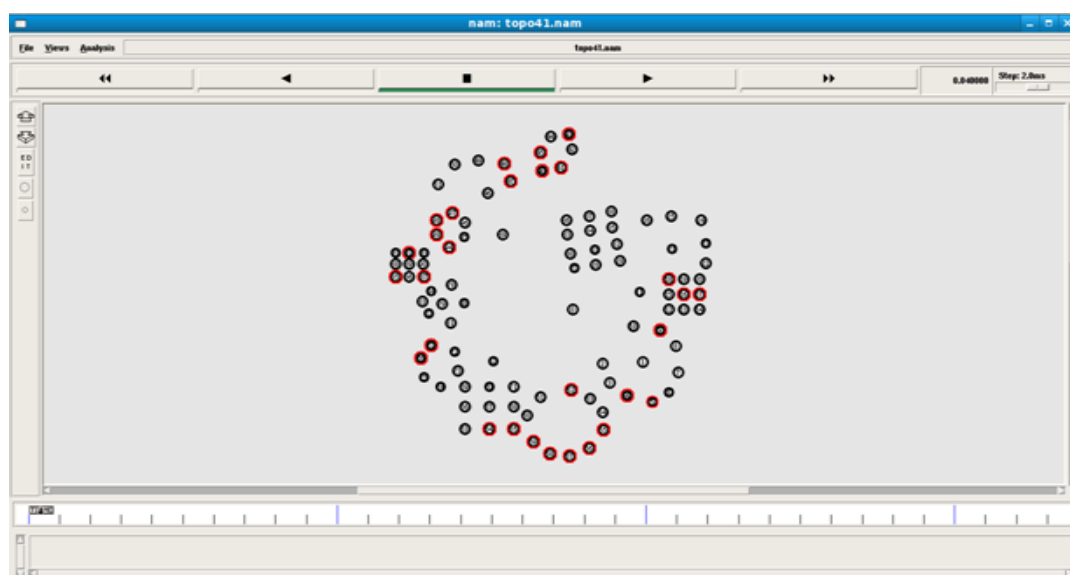


Figure 4: A snapshot of ITA result.

V. Conclusion

Calculation of the trust of the node helps in providing better reliability and security to the network. It improves the decision making process where the collected data play a major role. This method also helps in minimizing the rejection of the nodes due to fault identification thus ensuring optimum life time and usage of the nodes. The efficiency of the network increases due to the presence of trusted nodes alone. It can be implemented in real time environment to test against real time application to provide secure system for various applications.

VI. References

- [1]. B.A.Sabarish, M.Priyanka, G.Agalya, Sarayu.S. ITA: Improved Trust Architecture for Wireless Sensor Networks. International Conference on Electrical Engineering and Computer Science, ISBN: 978-93-82208-43-3.
- [2]. Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. In IEEE transaction on dependable and secure computing, March/April 2012.
- [3]. H. Zhu, F. Bao, and K. Kim. Computing of Trust in Wireless Networks. In 60th IEEE Vehicular Technology Conference, Los Angeles, California, September 2004.
- [4]. M. Blaze, J. Feigenbaum, and A. D. Keromytis. KeyNote: Trust Management for Public-Key Infrastructures (position paper). Lecture Notes in Computer Science, 1550:59–63, 1999.
- [5]. M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In IEEE Symposium on Security and Privacy, 1996.
- [6]. Miloš Blagojević^{1,2}, Majid Nabil, Marc Geilen¹, Twan Basten^{1,2}, Teun Hendriks², Marcel Steine¹: A Probabilistic Acknowledgment Mechanism for Wireless Sensor Networks. 1 Eindhoven University of Technology, the Netherlands 2 Embedded Systems Institute, Eindhoven, the Netherlands.
- [7]. Renjian Feng *, Xiaofeng Xu, Xiang Zhou and Jiangwen Wan: A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory. School of Instrument Science and Opto-electronics Engineering, Beijing University of Aeronautics and Astronautics (Beihang University), Beijing 100191.
- [8]. S.Karthik, K.Vanitha, Dr .G.Radhamani: Trust Management Techniques in Wireless Sensor Networks: An Evaluation. School of IT & Science, Dr.G.R.Damodaran College of Science, Bharathiar University, Coimbatore-641014, India.
- [9]. Seyed Hossein Hosseini Nazhad, Rasim M. Alguliev, Jalil Jabari Lotf: A Survey of Wireless Sensor Networks. University of ANAS Baku, Azerbaijan Republic.
- [10]. Vijay Varadharajan, Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun and Abdul Sattar: A Trust Management Architecture for Hierarchical Wireless Sensor Networks. Department of Computing, Macquarie University, Sydney, Australia janson, mehmet, rshankar, vijay}@science.mq.edu.au School of Information and communication Technology, Griffith University, Brisbane, Australia.
- [11]. Y.H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust Management for Web Applications. Computer Networks and ISDN Systems, 1997.