International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

To Prevent Internal Attack in Trust Model for Wireless Sensor Networks.

U. L. Prajapati[1] , R.R. Sedamkar[2] , K. A. Bhandari[3]
[1,2,3] *Thakur College of Engg. and Tech., Mumbai -400101, Maharashtra, India*

Abstract: Security is the one of the main concern in Wireless Sensors Networks (WSNs), And they are likely to be affected by many security threats, and because of multiple factor like communication, computation and to put off until a later time of WSNs, traditional security mechanisms cannot be used. Trust models have been recently suggested as a tool to produce a decisive effect on security mechanism for Wireless Sensor Networks (WSNs). Considerable research has been done on modeling trust. To calculate nodes trust value communicational behavior is taken into consideration by many researchers, which is not enough for trust evaluation due to the widely diffused malicious attacks on wireless sensor networks. Calculation of direct and recommendation trust are done by considering the numbers of packet received by sensor nodes. Firstly the direct trust is calculated by considering communication trust, data trust and energy trust. Trust reliability and intimacy are defined to improve the accuracy of recommendation trust.
In this paper best energy route is selected, here at the time of route request it can estimate total possible route with least hop count and best energy. Attacker node can give fake energy, in these via fake energy message it can hack route and get all packets. Trust model is built to prevent hacker. Our work will enhance the security of previous implemented trust model do perform the same vampire attack is been proposed. Vampire attack who actually does not hack any packet but it will recommend taking long route and end-to-end delay rate is increased. For more security here we can use key sharing and grid pattern method to prevent hacker. The proposed Method can evaluate trustworthiness of sensor nodes more precise manner and prevent the security fortification more effectively.
Keywords:WSN.

I. INTRODUCTION

Wireless Sensor Networks is technologies that have been widely used and it is emerging with the rapid speed in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid, etc. However the nature of a sensor network, which is the wireless and resource-constraint, makes it an ideal medium for malicious attackers to encroach the system. Thus, security is extremely important factor for the safe application of WSNs.

Different security mechanisms which can be applied to avoid the security threats are authentication, confidentiality, cryptography and message integrity, these proposed method provide security for security threats like message replay, eavesdropping, and construction of messages. However, these approaches still suffer from many security

issues, such as denial-of-service (DoS) attacks and node capture attacks. Captured nodes cause the internal attacks which cannot be effectively solved by security mechanisms used for today's security solution. Security mechanism are very much effective for external attacks but not for internal attacks. There is only one way to establish secure communication between internal nodes that there should be trust among them, and this lead to a important fact to establish that trust model between the nodes and allowing them all to infer the trustworthiness of all the nodes present in communication network. Trust model has been developed mainly to build trust relation among the nodes of source and base and all the nodes between them. Wireless sensor network contains uniquely categorize sensors to read the surrounding condition such as environment and physical conditions such as pressure, sound, temperature, etc. to deliver the information through network to main location i.e. source to base station. Numbers of nodes which we place are much more, they are cheap, less power consumptive, small in size and resource constrained devices.

Main area in which wireless transmission medium lack are availability of limited resource on sensor nodes, their working environment, unreliable communication, ignored operations and adhoc deployment. Therefore protocols for these sensitive sensor networks should be designed with keeping their security, constraints and challenges in mind. In single-hop communication energy efficiency is not as good as in multi-hop communication.

Progress in development of wireless sensor networks got limelight when the development in the field of radio networks has been studied deeply and come out in front of the society. Wireless sensor networks consists many sensors which are placed over a distance in large geographic area, which help in sensing the air humidity, change in temperature etc. Sensors which are placed in networks communicate to each other in adhoc manner and connect back to a Base station. Base station acts as gateway for user to solve the issue of the network. WSN allows the communication between sensors and base station. Application of sensor networks is highly adaptable due to growing popularity as advances in power and processor, combined with new energy harvesting methods. Application of these sensor networks mainly attracted two key groups of world, one is commercial and other is military user. Readings of WSN are advantageous in making decision or gain some advantage, so it is important to note that the data obtained is confidential and un-modifiable. Designs of WSN are such that they consume less power and remain valuable of longer time period and the protocol used leaves them vulnerable to attack.

II. HISTORY OF EXISTING TECHNIQUES

Communication behaviour is one of the factors affecting the trust model. An Efficient distributed trust model proposed by J. Jiang, G. Han, F. Wang and L. Shu does not only includes the communication but also the routing and data behaviour of sensors placed in network. The main component of EDTM is one and multi hop trust. One and multi hop trust combining includes six component which is been divided into small module which are direct, recommendation, indirect, integrated, trust propagation and trust update

module[1]. Calculation of direct, indirect and recommendation trust are carried and the best energy efficient route is selected for the communication. Direct trust reflects the direct communication behaviour between neighbour nodes; recommendation trust is calculated after applying some filtration rule and filtered reliable recommendation are calculated. And when there is no direct connection between source and destination node indirect trust is calculated. One of the best outcomes of EDTM is that it is attack resistance and efficient trust model.

A. Betts, F. Meyer, F. Muller and S.Y. Zhu concentrated on security parameters designed for different layers which are network, application and data-link layer, and deeply studied the security breaches related to different functioning of WSN and their environment. Functioning involve routing, authentication and data aggregation in WSN [2]. These all can also be counted as drawbacks of WSN like computational ability, power efficiency and limited battery of sensor nodes placed in network. Assumption that the data which is lost during the communication is not usable or not contiguous is depending on probability and this lead to a risk in any sensitive data networks. So the result of the paper shows that the security parameters are not up to mark for sensor nodes to be use in highly sensitive scenario like military or commercial.

W. Tianhua and W.Na, proposed a trust model the trust value depending on the multi factors, which are communication quality, data similarity and energy to measure trust between two nodes. Direct trust is evaluated by the number of successful and unsuccessful interactions, similar or dissimilar data comparison and energy. Furthermore, they quantified weight of the each factor to decide a more reasonable measurement for trust value. Indirect trust is calculated when direct trust is lower than certain threshold and it is evaluated of direct trust matrix in CH. Direct trust calculated on the basis of interaction between nodes and the trust between the nodes depend on multiple factors [4]. But as the relation between the factors is not simple traditional model cannot be applied here. Generally relation between two factors is dividing into three classes that are promoted, opposite and correlated.

In this table symbol '+' plus means promoted relation between two factors, '-' minus means opposite relation and blank means uncorrelated relation. From the table we can conclude that when valid interaction increased, similar data will increase and when interaction increased, energy will be consumed more. Time which is an attribute of data has the same relation with other factors as data. It is blank between data and energy due to transitive of interaction, data and energy.

Table 2.1- Relationship between factors [4]

	Interaction	Data	Time	Energy
Interaction		+	+	-
Data	+			
Time	+			
Energy	-			

Z. Yo, D. Kim and Y. Doh provided a parameter and localized trust management scheme for sensor network security where trustworthiness of neighbour nodes are maintained by sensor node depending on highly abstracted parameter to adopt appropriate cryptographic method identify the malicious nodes and share the opinion locally. The main feature was to maximise the security and minimizes the energy consumption for sensor nodes in wireless sensor networks.

In PLUS the key design point is based on parameter database, trust estimator, network input/output, Routing operator and Security response. Wherein the parameter database includes management, visualization, exploration and availability. Frequently and infrequently changing parameters which can be network status, nodes local information and operational environment, application types respectively [5]. Trust estimator calculates the trustworthiness of the individual node. To calculate the same in the paper some definition are given, Judge: Who performs Evaluation. Suspect: Who all are in the radio range of judge and will be evaluated. Jury: Who maintains the trust value of suspect with judge and send out the corresponding opinion periodically.

A,S, Alkabani, A.O. Md. Tap and T. Mantoro, studied the popular and reputed trust models for WSNs. Main challenges during the routing of data is to maintain the power consumption, accuracy and scalability, high the power consumption shorter the life of network. Lack of research in trust and reputation model inspire them to compare between these two specially in terms of energy efficiency [6]. This paper presents comparison between several proposed trust and reputation models in terms of average path length, average accuracy and energy consumption rate. The LFTM model developed is suitable for static and oscillating WSNs whereas Power Trust is an optimized model to be used for dynamic WSNs because of its efficiency.

S. Singh, V. Varma and N. Pathak, has examined the impact of sensor augmentation parameter for static and dynamic WSN with trust and reputation models. In particular, they present a novel WSN framework-based investigation on peer trust and linguistic fuzzy trust model (LFTM) for trust and reputation models accuracy, path length, and energy consumption for sensor-node operations are reported for their current and average scenarios [7]. They computed accuracy and path length in terms of overall percentage of the functionality whereas energy consumption in terms of micro joule specifically for sensor node operations. They mainly focused on firstly the accuracy, path length, satisfaction and energy consumption for the path length value in both of the trust and reputation models stated above. Next the overall framework for comparative evaluation of trust and reputation model and lastly the same model is deployed for the overall evaluation of a wireless sensor network. Conclusion from the above models reflects their strong affection and correlation in static WSN mode.

G. Han, H. Xn, J. Jiang, L. Shu and N. Chilamkurti, have worked on the localization performance which is affected by radio irregularity model. There is high probability that unknown nodes cannot receive sufficient location message under the radio irregularity model. In order to improve localization accuracy a new 2-hop localization scheme is introduced by authors. Then they point out the relationship between degree of irregularity (DOI) and communication distance. And impact of radio irregularity on message receiving

probability. Simulation results shows that the increasing DOI and TR lead to larger localization error, proposed 2-hop localization scheme reduces the localization error and has better localization performance.

III. PROBLEM STATEMENT

Sensor nodes in sensor network are wireless and placed randomly these arrangement lead us to many breaches in sensor network and deployment nature arise unique threats, along with to maintain and guarantee the integrity, reliability and confidentiality of the sensor nodes over sensor networks. The growth in security prevention for WSN is very much appreciable but there are still these threats are danger and insufficient for the increasing growth and trust of the networks. Literature in the field of wireless sensor networks address a specific security issue but ignore other which drag us to level of security by achieving low energy and high memory consumption. After studying the various implementations of trust model and their behavior in the environment of wireless sensor networks a new system is suggested in this project which will try to overcome the security breaches of trust model for wireless sensor networks.

The proposed model will focus on implementing, enhancing, increasing the security mechanism in the wireless sensor networks behavior and communication. On basis of attack, maintaining the authenticity, originality and integrity of information we have to prevent the attack and select the best communication route. To add up to the more security different method can be used to confuse the attacker node**.**

IV. PROPOSED IDEA

The entire research work could be broken down into the following modular sections:

- Best Energy Route Selection
- Attacker
- Trust Model
- Vampire attack

Whenever the Communication between subjective and objective node is establish one of the main concern is about the amount of energy consumed during the entire process of transfer of information minimum the energy consumed better the model is rated. Here in the proposed model at the time of route request it can estimate the total possible route with energy needed to perform the task. After evaluation of the entire possible available route the best route with least hop count and best energy.

To deal with attacker a fake attacker node is being created. Fake attacker node give the fake energy message to attacker node and via this fake energy message it can hack the route and get all the packets.

The implementation of trust model is being planned in this module. Trust model will prevent the hacker from hacking the message while passing the information from the subjective node to objective node.

In this module a vampire attack is planned which actually does not hack any packet but it will recommend to take long route for message delivery and end to end delay rate is

increased in the communication.

V. EXPECTED RESULTS

Our experiment uses ns2 to design. Fifty nodes are distributed in space of 100×100, and the communication radius will be around 50. As the energy efficiency is one of the main aspect in sensor network the various graphs that we are going to measure is packet delivery ratio with respect to time, which will take in the consideration efficiency of the communication within the sensor network. The other graphs that will be measured are throughput, delay, energy and overhead with respect to time. Graphs of the energy with respect to time are calculated by varying the percentage of malicious nodes on regular interval of time. Proposed system will consume lower energy will take less memory space because nodes in the sensor network does not keep information about all node in network but only keep the information about the neighbour nodes

REFERENCES

i. J. Jiang, G. Han, F. Wang, L. Shu and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 1228- 1237, May 2015.

ii. Y. Lu, K. Lin and K. Li, "Trust Evaluation Model against Insider Attack in Wireless Sensor Networks," in *IEEE Second International Conference on Cloud and Green Computing (IEEE Computer Society)*, pp.319-326, Dalian, China, 2012.

iii. A. Betts, F. Meyer, F. Muller and S.Y. Zhu, "Wireless Sensor Network Security: A Critical Literature Review," in *IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems (COMCAS 2013), Tel Aviv, Israel*, 21-23 October 2013

iv. 4 W. Tianhua, W.Na, "A Trust Model for Wireless Sensor Networks based on Multi-Factors," In the 9th *International Conference on Computer Science & Education (ICCSE 2014),* Vancouver, Canada, August 2014.

v. Z. Yao, D. Kim and Y. Doh, "PLUS: Parameterized and Localized trUst Management Scheme for Sensor Networks Security," in *Proc. IEEE Int. Conf. Mobile adhoc Sensor syst*., 2008, pp. 437-446.

vi. A,S, Alkabani, A.O. Md. Tap and T. Mantoro, "Energy consumption evaluation in trust and reputation model for wireless sensor networks," in *IEEE 5th International conference on information and communication technology for muslim world. Malaysia 2013*.

vii. S. Singh, V. Varma and N. Pathak, "Sensor Augmentation Influence Over Trust and Reputation Models Realization for Dense Wireless Sensor Networks," *IEEE Sensors Journal,. Vol. 15, No. 11, November 2015*.

viii. G. Han, H. Xn, J. Jiang, L. Shu and N. Chilamkurti, "The Insight of Localization through Mobile Anchor Nodes in Wireless Sensor Networks with Irregular Radio," *KSII Transaction on Internet and Information System*, vol.6, No. 11, Nov 2012.

ix. V. Umarani and K. Sundaram, "Survey of Various Trust Models and their Behaviour in Wireless Sensor Networks," IJETAE, volume 3, Issue 10, October 2013

