IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 50-54
www.iosrjournals.org

Prevention of Attack in WSN using Certificate Revocation

U. L. Prajapati[1], Dr. R.R. Sedemkar[2].
[1]*M.E Student, Computer Engineering Department, Thakur College of Engineering & Technology, Mumbai, India*
[2]*Dean. Professor, Computer Engineering Department, Thakur College of Engineering & Technology, Mumbai, India*

Abstract-*Wireless Sensors Networks (WSNs) are susceptible to many security threats, and because of communication, computation and delay constraints of WSNs, traditional security mechanisms cannot be used. Trust models have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). Considerable research has been done on modeling trust. However, most current research work only takes communication behavior into account to calculate sensor nodes' trust value, which is not enough for trust evaluation due to the widespread malicious attacks. According to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust.*
In this paper,firstly best energy route is selected, and to eradicate the security threats an efficient certificate revocation scheme is adopted. After that in second step to attain secure communication,instead ofdirect trust value it takes into consideration the recommended trust.A conventional scheme in WSNs aims to achieve greater security by electing a Cluster Head (CH) for each cluster which governs the entire network. To achieve the goals, here a Vectorbased trust mechanism (VBM) is introduced which nominates a CH based on the higher trust value computation with earliest bit vectors and Certificate Revocation scheme (CR) for discarding the authorization of the misbehaving nodes. This method achieves greater reliability, consumes less energy, avoids false accusation, quicker revocation time and efficient trust value computation, and also reduces the communication and computational costs compared to the existing mechanism which is EDTM model. Our simulation results express that the proposed mechanism yields an exemplary outcome for providing secure transmission in WSNs. The proposed Method can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more effectively.

Index Terms-*Wireless sensor networks, Energy efficient, Trust model, Certificate Revocation.*

I. Introduction

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

Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trustworthiness of another node. Nowadays, many researchers have developed trust models to build up trust relationships among sensor nodes. Wireless sensor network (WSN) consistsof spatially distributed autonomous sensors tomonitor physical or environmental conditions,such as temperature, sound, pressure, etc. tocooperatively pass their data through thenetwork to a main location. A WSN is composedof tens to thousands of sensor nodes, which arelow-power, low-cost, small, resource constraineddevices. Using a narrow radiocommunication range, a sensor node wirelesslysends messages to a base station via a multihoppath.

Wireless transmission medium,limited resources available on sensor nodes,hostile environment, adhoc deploymentunreliable communication, and unattendedoperation. Therefore, protocols for criticalsensor networks should be designed withsecurity in mind, while taking into considerationtheir specific constraints and challenges. Forlarge sensor networks, multi-hopcommunication is more energy-efficient thansingle-hop communication.

Recent developments in the field of radio networks have given light to the creation of wireless sensor networks (WSN). These are made up of many wireless sensors spaced over a geographic area, which perform a particular task such as sensing air humidity. The WSN allows these sensors to communicate in an ad-hoc fashion to adaptively connect sensors back to a Base Station which acts as a gateway for users to query the network. The popularity of these sensor networks is growing exponentially as advances in processor and sensor power use, combined with new energy harvesting methods allow sensors to be highly adaptable to their applications. Interest originates from two key groups, commercial and military users. Organizations rely on WSN readings to make decisions or gain advantage, so it is essential that this data is not modifiable and remains confidential. The protocols used in WSNs are fundamentally designed to utilize the lowest possible power, to ensure longevity of the WSN, leaving them vulnerable to attack. This report investigates a key technology at each layer of the network; covering data aggregation, routing protocols and user authentication.

II. Related Work

J. Jiang, G. Han, F. Wang and L. Shu, proposed An Efficient distributed trust model which not only consider the communication behavior but also the routing and data behavior of the sensor nodes. EDTM consist of two main components: one-hop trust and multi-hop trust model which include following six components: direct trust module, recommendation trust module, indirect trust module, integrated trust module, trust propagation module and trust update module [1]. In EDTM structure three different trust is been calculated, Direct trust, Recommendation trust and Indirect trust. Direct trust is a kind of trust based on the direct communication behavior. It reflects the trust relationship between two neighbor nodes. Since the recommendations from the third parties are not always reliable, they have used efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust. In the absence of connection between subject and object node indirect trust is calculated based on the recommendation from the other nodes. Trust model can assist in many applications such as secure routing, secure data aggregation and trusted key exchange. An efficient trust model is required to handle trust relation in secure and reliable way.

S.J. IndhuLekhaand R. Kathiroliproposed Vector Based Mechanism which aims to spot the malicious node with the trust vector bits and revocate the authorization using ECR. This proposed scheme achieves efficient detection of misbehaving nodes which leads to reduced revocation time and solves the false accusation problem without affecting the freedom of the accuser [2]. Energy is a prime factor for the nodes in the MANET. This scheme reduces the energy intensity of the nodes with low communication and computational overhead.

Nirwan Ansari proposed a cluster based certificate revocation scheme where nodes are organized to form clusters. In this scheme a certification authority issues and revokes the certificates of the nodes by maintaining warning list and black list [3]. If the nodes act maliciously then the neighbor node will accuse it to CA (certificate authority) and the nodes are placed in blacklist. The CA will send the accusations to CH to confirm that the nodes in the blacklist are malicious are not. If CH confirms then the certificate of malicious nodes are revoked. Else the nodes are recovered from malicious list to warning list. To enhance accuracy and to improve the reliability, the warned nodes take part in the certificate revocation. The communication overhead is very high in this scheme.

JoiyonCiulow proposed the decentralized suicide based approach. In this approach, the certificate of malicious nodes can be quickly revoked with just an accusation by the neighbor node [11]. But, not only the certificate of the accused node but also accuser's certificate will be revoked. At least one node has to sacrifice itself to remove an attacker from the network.

R.Venkataraman,Proposed a trust model is incorporated over ad hoc on demand distance vector routing protocol and efficient link state routing protocol in MANETS. The performance evaluations show that by carefully setting the trust parameters, an efficient throughput can be maintained with minimum overhead [5]. The computed trust and confidence values are introduced into the path computations process of the ad hoc routing protocols. It was observed that the node in the network were able to learn the malicious activities of their neighbors and hence alternate trustworthy paths are taken to avoid data loss in the network with trade off in end to end packet delay and routing traffic.

Insider attack is one of the key attacks in wireless sensor networks. Y. Lu, K.Lin, K.Li proposed a novel trust evaluation model to enhance the data security in WSNs [4]. In the proposed design each node computes the trust value of its 1-hop neighbors based on their multiple behavior evaluation with no requirement on a prior knowledge about normal/compromised sensor activities and builds a trust management. Trust management exploits the spatial correlation among the networking behaviors of sensor in close proximity of each neighbor node. The simulation result gives the positive sign of high performance in combating insider attack. One of the positive things of the research is it does not require knowledge about faithful and compromised sensors, which is important with considering the dynamic attacking behaviors. Further this trust

model can be employed to the routing algorithm with multiple attributes evaluated simultaneously. High security and performance is achieved by adjusting the parameter about the trust value and energy.

A. Betts, F. Meyer, F. Muller and S.Y. Zhu, studied the Security mechanism designed for data-link, network and application layers, and also investigated the security vulnerabilities associated with the data-aggregation, routing and user authentication in WSN environments [6]. In the paper they have concluded that Limited battery and computational abilities of sensor nodes leads data aggregation technologies to focus on power efficiency, accepting that some data is going to be compromised and relying solely on probability in the hope that lost data is not contiguous or useable. This paradigm poses an unacceptable risk to any sensitive data networks. At the network layer, all major routing protocols are equally flawed, generally overlooking security. The only acceptable progress is in the form of INSENS, which increases network resiliency to traditional attacks but induces high computational requirements and is still exploitable by new attacks. Finally, at the application layer, protocols implementing biometric cryptography show promise for user authentication; although, the costs and weaknesses of such deployments are currently unknown. These discoveries indicate that a motivated attacker will be able to break any current WSN, leading this paper to ultimately conclude that these networks are not suitable for any military or commercial use where the security of data is an operational concern.

III. Exciting System

In the existing methods, they used various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we need to ensure that all communicating nodes are trusted. Most existing studies only provide the trust assessment for neighbor nodes. Moreover, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes.

IV. Proposed System

In this paper, we propose a trust model for improve security. The proposed model can evaluate the trust relationships between sensor nodes more precisely and can prevent security breaches more effectively. This paper is a multi-hop network which means that the sensor nodes can only directly communicate with the neighbor nodes within their communication range. The packets exchanged between any two non-neighbor nodes are forwarded by other nodes. Theforwarding node can not only send the data from source nodes to destination nodes but also can process the information based on their own judgments. Generally, the trust value is calculated based on recommendations from a third party and on the basis of revocation certificate given by cluster authority to each cluster members. The third party who provides recommendations is a recommender and also revokes a certificate for each neighbor node from source to destination. Clustering is being used for better performance as increase in network size result in degradation of performance.

4.1 System Architecture

A centralized Cluster Authority (CA) manages certificates for all the nodes in the network, cluster construction is decentralized and performed autonomously. Nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are located within the communication range of their CH. Each CM belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster. Clustering information is never used for routing; it is only used for managing certificates in the certification system. This provides a clear advantage as it enables the scheme to be used along with any type of routing technology. The aim of using clusters is to enable CHs to detect false accusations. Requests for the CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, only in the case where it is a CM in its cluster.In other words, a CH will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not. Since the CA regularly broadcasts certificate information on nodes which have been accused as malicious nodes, CHs will be able to detect false accusations against their CMs by comparing this information with their own local observations. In order for clustering-based certificate revocation to work, CHs must be legitimate. Nodes can be classified into three different categories, normal nodes which are highly trusted, warned nodes with questionable trust, and attacker nodes which cannot be trusted. Only normal nodes are allowed to become CHs and accuse attackers by sending Attack Detection Packets (ADPs) to the CA. Nodes in the Warning List (WL) cannot become CHs or accuse attackers, but they can still join the network as CMs and communicate without any restrictions. Nodes classified as attackers are considered malicious and completely cut off from the network. The reliability of each

node is determined by the CA as follows. The CA maintains both a Black List (BL) and a Warning List. When the CA receives an ADP from an accuser, the accused node is regarded as an attacker and is immediately registered in the BL. The BL includes nodes which are classified as attackers and have had their certificates revoked.

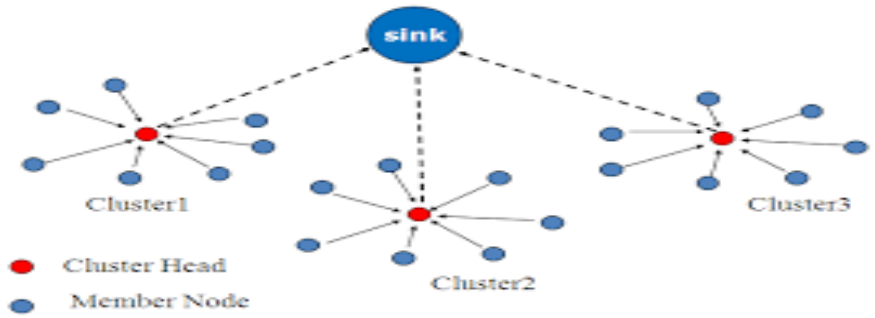

Fig 1. System architecture of proposed system

V. Simulation Results

Here, we analyze the detection performance to verify the effectiveness of our method. The curve of the various parameters describes the trend in contrast to the previous method. The detection time represents the amount of time needed to detect all malicious nodes in the network. By using the previous method, as expected in our analysis, when the number of malicious nodes is less than a specified value (40 in this simulation), the scheme works well.

To evaluate the detection performance of the scheme, we study the impact of various parameters related to each other. In figure 1 we can see the graph of packet interval vs control overhead the comparison is made with routing protocol APTEEN. The red colored graph indicate the traditional control overhead packet and the one in green color is after applying revocation on the model already exists. In the graph at each point we get better result than original cluster overhead.

Figure 2 give us the graph of dropping ratio of packets while communicating from source node to destination node.

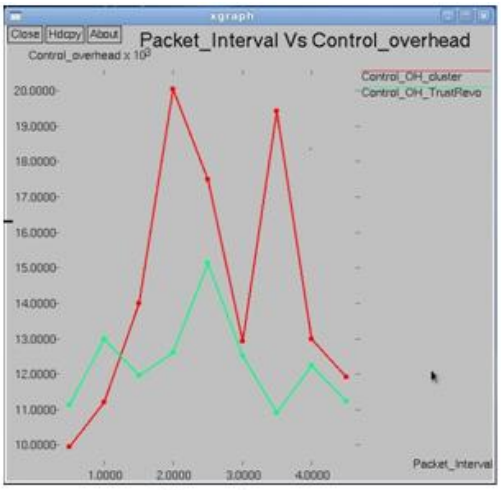

Figure 1.

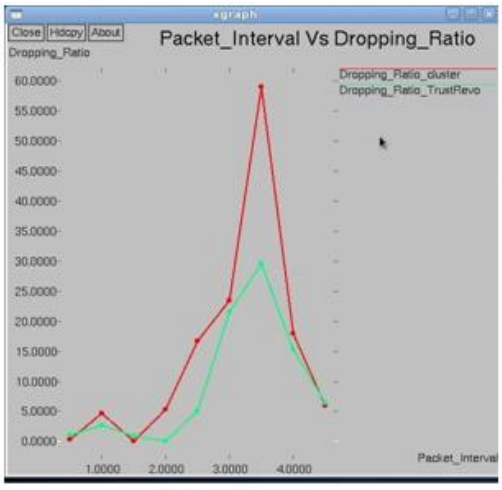

Figure 2.

Next graph which is shown in figure 3 is graph of comparison between packet interval and delay. After applying the trust revocationmethod we got better result than normal clustering techniques.

Figure 4 compare the packet interval with PDR and results in better performance than normal technique. And the graph of packet interval and average energy is shown in figure 5. This gives slight low result as compare to clustering technique at the start of packet transfer but as the number of packets increases result get better.

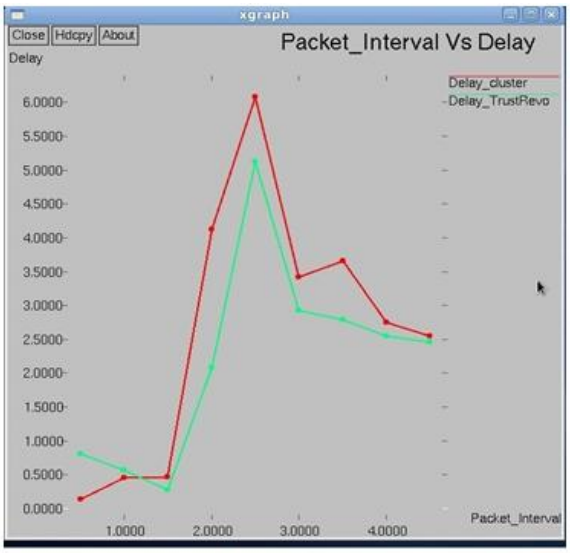

Figure 3.

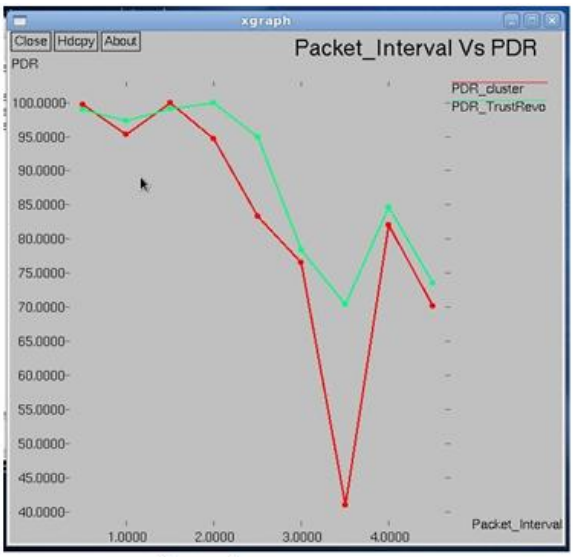

Figure 4.

VI. Conclusion

In WSNs, security has the paramount importance due to the dynamic, infrastructure less and unpredictable nature of the nodes in the network. Our proposed trust model with introduction of certificate revocation aims to spot the malicious node with the trust vector bits and revocate the authorization using CR. This proposed scheme achieves efficient detection of misbehaving nodes which leads to reduced revocation time and solves the false accusation problem without affecting the freedom of the accuser. Energy is a prime factor for the nodes in the WSNs. So our scheme reduces the energy intensity of the nodes with low communication and computational overhead. Our simulation results indicate that our novel mechanism provides a good outcome compared to the traditional ones, which is clustering.

References

[1] 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.

[2] S.J. IndhuLekha, R. Kathiroli, "Trust Based Certificate Revocation of Malicious Nodes in MANET", *2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 2014.

[3] Nirwan Ansari, Jie Yang, and Nei Kato, Wei Liu, Hiroki Nishiyama, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", *IEEE transactions on parallel and distributed systems*, vol. 24, no. 2, February 2013

[4] 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.

[5] R. Venkataraman,M.PushpalathaT,RamaRao,"Regression-based mobile adhoc networks", *IETInf.Secur. 2012*, vol.6, Iss.3, pp.131-140.

[6] 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.

[7] 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.

[8] 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.

[9] 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.*

[10] 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.*

[11] Jolyon Clulow and Tyler Moore, "Suicide for the Common Good: a New Strategy for Credential Revocation in Self-Organizing Systems*" ACMSIGOPS Operating Systems Reviews*, vol. 40, no. 3, pp.18-21, .luI. 2006.

[12] 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.

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