World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-4, Issue-4, April 2017 Pages 49-51

Review On: Approaches for Excluding Compromised Node by Evaluating Trust in Wireless Sensor Network

Ravneet Kaur, Priyanka Mehta

Abstract— This paper analyse the enhancements in excluding compromised nodes using AES key encryption sign for identification in wireless sensor network. The wireless sensor networks (WSN) are specialized transducers with spatially dispersed and dedicated autonomous sensor nodes for identifying, monitoring and recording the physical and environmental conditions at different locations. Different trust systems have been proposed to reduce the effect of routing attacks, but most of them could not determine the malicious node effectively and some of them suffer from the attacks on the system. In this paper, we propose a security of wireless sensor network by excluding the black node and compromised nodes. using authorization and encryption and exclude compromised node by evaluating the trust factor in wireless sensor network. The main Emphasis of our research is on to check the trust factor of node from centralized server i.e. Cluster head which control the whole network to prevent the problem of black node.

***Index Terms*— Networks, Authorization, Encryption, Cryptography, Authentication etc.**

I. INTRODUCTION

The wireless sensor networks (WSN) are specialized transducers with spatially dispersed and dedicated autonomous sensor nodes for identifying, monitoring and recording the physical and environmental conditions at different locations. Of the most commonly monitored physical parameters include temperature, pressure, light, direction of wind and its speed, intensity of illumination, vibration and sound, chemical concentration in water, air, pollutant level, humidity, vital body functions and so on.

WSN is a revolutionary technology that comprises of several sensor nodes that are small in size, light in weigh and easily portable. These sensor nodes are laced with a radio transceiver, a microcontroller and a battery, which can either be embedded in it or located externally as an energy resource.

This hi-end information gathering technology was originated as an initiative of keeping surveillance checks in the wars or battlefields. With its great potential applications, today, it is widely and effectively deployed in wide-mission vital military operations, various industries monitoring the health of machineries, agriculture and commercial domains for monitoring and controlling various other applications. As the WSN deals in highly sensitive information, its processing, gathering and transmittance, therefore, security in this spatially dispersed nodal network is of crucial concern. This kind of highly sensitive data, which can be related to a patient for its medical background data, military operations related strategies or highly confidential mission data, data related to earthquake, or other such environment calamity and much more must be dispersed or transmitted in an encrypted format. As any leakage or misuse of this critical information or data can create serious issues and impact an individual or the entire nation badly, thus, it becomes of paramount importance to secure the data of the sensory nodal network by deploying effective and efficient network security techniques.

The sensor nodes of WSN work under extreme resource constraints as the energy resource usually comprises of an embedded device with limited supply to transmit data in a highly unspecified environment. Being a wireless mode of network, the chances of data packets getting damaged due to an unwanted error, or conflict amongst the nodes or over congestion is very high. As the entire security mechanism of the network depends upon the cryptographic key distribution and reporting of critical events, the unreliable mode of communication amongst the sensor nodes poses grave threat to the security of the network. Additionally, sending and receiving secure data in highly callous conditions is not an easy task as the sensor nodes have the tendency to closely interact with their physical environment to process and blend data and create novel information that must be transmitted to the end-station. However, these uncontrolled operations in unattended environment may create accidental node failure.

The security of Wireless Sensor Network (WSN) is effected due to the attacks on the sensor nodes, which are often categorized as goal-oriented attacks, and performer-oriented attacks. Goal-oriented attacks are mainly against the data confidentiality wherein an attacker passively monitors the traffic, analyzes it for imperceptibly encrypted sensitive information and then gains authentication information to pass through the network. This type of attack is called passive attack which results in the revelation of sensitive information to the attacker without any knowledge at the user's part. However, in the active attack, the attacker actively assesses the entire network to gain control over it. The best and most common ways of active attack includes data modification, spoofing, sinkhole, flooding, jamming the network, warm hole, black hole, fabrication, lack of co-ordination, node subversion, false nodes, selective forwarding and so on. While in performer-oriented attacks, the attacks are either internal or external. Internal attackers

Ravneet Kaur,Department of Computer Engineering ,Universal Campus, Lalru (SAS Nagar), Punjab,India
Priyanka Mehta, Department of Computer Engineering ,Universal Campus, Lalru (SAS Nagar), Punjab,India

are the trickiest ones as they are not only the legitimate node of the original network but also have direct access to all the sensitive network information. The internal attacks include modification, misrouting, eavesdropping and packet dropping attacks that leads to suppression of critical information reaching the base station, thereby degrading the network performance.

II. Proposed Work

The main Emphasis of our research is on to check the trust factor of node from centralized server i.e Cluster head which control the whole network to prevent the problem of black node.In this, according energy consumption and trust value,we will make the cluster head using highest energy and higher trust value. The node that have lowest enrgy and lower trust value, Base station will send an encrypted message to That particular node and, user will decrypt the message, if the decrypted message matched to original message then Base station automatically increase the trust value otherwise,it will declared as Compromised Node and Base station will exclude this node from the network.For preventing the black node we have following rules to build up the wireless Sensor Network

A. Authentication phase:

For fresh node ,there will be two phases to join the network :: in authentication phase server will check some unique parameters If all parameters are matched then authentication is done and server will send a encrypted message to Client.

B. Excluding Phase:

In authorization phase user will decrypt the message received by server using its key and send to the server, if decrypted message is matched with the sending message then authorization phase is done and

user will be logged in. For communication there will be key agreement phase between two users, so by this black node will be unable to communicate into the network. we make cluster head with the help of energy and with highest trust value that will check every node trust factor and exclude all the black nodes. File sharing will be using encryption method so that if black users receive this file will be unable to decrypt this file.

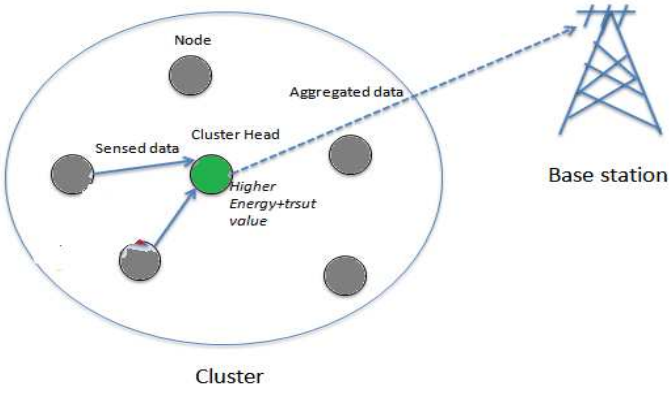

Fig 1: Distribution of cluster head in multiple nodes

III. Literature Survey

Weidong Fang, Chuanlei Zhang, Zhidong Shi, Qing Zhao, and Lianhai Shan [1] in their research study "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks" proposed The Beta-based Trust and Reputation Evaluation System (BTRES) for WSN's node trust and reputation evaluation. BTRES was based on monitoring nodes' behavior, and beta distribution was used to describe the distribution of nodes' credibility. The node trust values were used to guide the selection of relay nodes, mitigating internal attacks risks. Simulation results showed that the use of BTRES could effectively maximize the defense of internal attacks from compromised nodes and improve the WSNs' information security.

Yun Liu, Chen-xu Liu, Qing-An Zeng [2] in the research work "Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks" proposed an improved trust management method for data aggregation based on the relationship between nodes that was called the strength of the ties between the nodes. The improved method was developed from the trust model in the iRTEDA protocol and increasing the utilization efficiency of second-hand information coming from neighboring nodes. The aim of the proposed trust model was to obtain a higher level of security for data aggregation and the results showed that data aggregation based on trust management method could get higher accuracy of evaluating nodes' trust and reputation and achieve higher data accuracy of aggregating.

Vinod Kumar Verma, Surinder Singh, N. P. Pathak [3] in their research study "Towards comparative evaluation of trust and reputation models over static, dynamic and oscillating wireless sensor networks" proposed pervasive explorations of wireless sensor network to investigate the effect of static, dynamic and oscillating modes. The model constituted five trust and reputation models namely: bio-inspired trust and reputation, Eigen trust, peer trust, power trust, linguistic fuzzy trust and reputation. The impact of different wireless sensor networks modes had been judged for accuracy, path length and energy consumption over deployed models.

X. Anita, M. A. Bhagyaveni, J. Martin Leo Manickam [4] in their research study "Collaborative Lightweight Trust Management Scheme for Wireless Sensor Networks" proposed a collaborative lightweight trust-based (CLT) routing protocol for WSNs with minimal overhead in regard to memory and energy consumption. It did not use promiscuous mode of operation to monitor the neighboring nodes for trust derivation. CLT employed a novel trust counselor that monitored and warned the neighboring nodes whose trust fell below a warning threshold. The warning message alarmed a sensor node to check and correct the packet forwarding behavior to improve its trust relationship with its neighbors.

Yannis Stelios, Nikos Papayanoulas, Panagiotis Trakadas, Sotiris Maniatis, Helen C. Leligou, and Theodore Zahariadis [5] in their research paper "A Distributed Energy-Aware Trust Management System for Secure Routing in Wireless Sensor Networks" proposed a secure routing solution based on a novel distributed trust management system, which allowed for fast detection of a wide set of attacks and also incorporated energy awareness. This model showed efficient detection of malicious nodes and retained connectivity even when malicious nodes represented 72 per cent of the existing nodes.

Monia, Sukhchandan Randhawa and Sushma Jain [6] in their research study "An Efficient Trust Management Algorithm in Wireless Sensor Network" proposed a simple and efficient algorithm that calculated the value of the trusted node and found the malicious node. An improved algorithm was proposed that selected the nearby cluster head on the basis of the received signal and calculated the trust value on the basis of the packet forwarding factor. They analyzed the consistency of clusters and lifetime of the network.

Geetha D. Devanagavi, N. Nalini, Rajashekhar C. Biradar [7] in their research study "Trusted Neighbors Based Secured Routing Scheme in Wireless Sensor Networks Using Agents" proposed an agent based Secured Routing using Trusted neighbors (ASERT) in WSN. ASERT selected trustworthy neighbors and established secured routes using software agents. Agents effectively performed the function of finding trusted neighbors using probability based trust model and MAC model ensuring higher security and hence the secured routes were established. Two phases were involved in identifying trusted neighbors: in the first phase, agents visited all the neighbors and brought probability of all the neighbors using trust model and in the second phase, agents ensured the trusted neighbors using MAC model.

IV. Research Gaps

The above study of this research topic overcome the different research points of different researchers on the topic of wireless sensor network prints matching based on their minutiae and the correlation of different points of the trust value. In this the different authors works on different techniques to find the compromised node of wireless sensor by evaluating trust factor.

Many of the research paper worked only on the prevention of black node, but not on the find the compromised node and excluding them from the wireless sensor network.

The existing research study has a big drawback in terms of not explaining the role of centralized server i.e Cluster head in checking the trust value of the nodes. Despite centralized server being the main controller of the entire network, the decision of nodes communicating with each other is based on the information received from the adjacent node. In such cases, presence of a black node in the network can cause severe damage to the network. Therefore, a black node can pose a big threat if the centralized network fails to detect its entry in the network, joining and connecting with other nodes as black node is known for sending wrong information to other nodes, thereby affecting the trust value of the target node as a whole.

In this work I have removed the identification problem on the based on AES encryption.

.

V. Conclusion

There are multiple reputation techniques available to detect the black nodes and compromised nodes. Research paper worked only on the prevention of black node, but not on the find the compromised node and excluding them from the wireless sensor network. . Trust factor and trust management system being a highly recommended way to secure the sensor nodes and their transmissions of data, is studied and designed by many researchers in the past to clear the obstacles in the wireless sensor network. In this, we have worked on the compromised node using AES enhancements in encryption with homomorphic and maintained the energy level using enhanced AES algorithm. Trust value is the main factor to maintain the security and privacy of each node. File sharing will be done on the basis of key ,so there is no chance of inconsistency of file . We suggest for future work to provide an efficient algorithm for find and optimize the topologies' dynamically.

References

[1] Jun-Won Ho, Wright .M, S.K. Das, "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing," IEEE Transactions on Dependable and Secure Computing, Vol. 9, no. 4, pp. 494 - 511, July/August 2012.

[2] T. Abuhmed, N. Nyamaa, and D. Nyang, "Software-Based Remote Code Attestation in Wireless Sensor Network," Proc.IEEE GLOBECOM, Dec. 2009.

[3] T. Park and K.G. Shin, "Soft Tamper-Proofing via Program Integrity Ver-ification in Wireless Sensor Networks," IEEE Trans.Mobile Computing, vol. 4, no. 3, pp. 297-309, May/June 2005.

[4] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT:SoftWare-Based Attestation for Embedded Devices," Proc. IEEE Symp. Security and Privacy (S& P), May 2004.

[5] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Distributed Software-Based Attestation for Node Compromise Detection in Sensor Networks," Proc. IEEE 26th Int'l Symp. Reliable Distributed Systems (SRDS), Oct. 2007.

[6] Mathews .M, Min Song, Shetty .S, McKenzie .R "Detecting Compromised Nodes in Wireless Sensor Networks," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Vol .1, pp. 273-278 August 2007.

[7] Bose, P. Morin, I. Stojmenovic, J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks", *ACM Wireless Networks*, vol. 7, no. 6, pp. 609-616, 2001.

[8] A. Dahbura, K. Sabnani, L. King, "The comparison approach to multiprocessor fault diagnosis", *IEEE Trans. on Computers*, vol. C-36, no. 3, pp. 373-378, 1987.

[9] J. Deng, R. Han, S. Mishra, "Security support for in-network processing in wireless sensor networks", *2003 ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03)*, 2003.

[10] J. Deng, R. Han, S. Mishra, "A Robust and Light-Weight Routing Mechanism for Wireless Sensor Networks", *Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS)*, 2004.

[11] W. Du, J. Deng, Y.S. Han, P. K. Varshney, "A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks", *IEEE 2003 Global Communications Conference (GLOBECOM)*, 2003.

[12] W. Du, J. Deng, Y.S. Han, P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", *10th ACM Conference on Computer and Communications Security'03)*, 2003.

[13] Michael L., Simon A.C., Ruth M., Kathleen J., "Truth Machine: The Contentious History of DNA Fingerprinting", University of Chicago Press: Chicago, (2008)

[14] Soni N., Siddiqua A., " Filtering Techniques used for Blurred Images in Fingerprint Recognition", International Journal of Scientific and Research Publications (ISSN 2250-3153), Vol. 3 (Issue 5), May 2013 .

[15] Amrita Ghosal and Jyoti Prakash Singh "Secure Data AggregationUsing Some Degree of Persistent Authentication in Sensor Networks"Proceedings of the Conference on Mobile and Pervasive Computing(CoMPC-2008), pp. 183-186, August 2008.

[16] Aravind Iyer, Sunil S. Kulkarni, Vivek Mhatre and Catherine P.Rosenberg "A Taxonomy-Based Approach to Design of Large-Scale

[17] Sensor Networks", proceedings of the Conference on Wireless SensorNetworks and Applications, Signals and Communication Technology,pp. 3-30, 2008.

[18] Banerjee, I., Chanak, P., Sikdar, B.K. and Rahaman, H. "EER:Energy Efficient Routing in Wireless Sensor Networks", Proceedings of the IEEE Students' Technology Symposium (TechSym) pp. 92-97, Jan 2011.

[19] Algorithms",Proceedings of the IEEE Workshop on High PerformanceSwitching and Routing (HPSR'04), Phoenix, pp. 241-245, April 2004.