A systematic review for secure node authentication in Wireless Sensor Network

Jatinder kaur
Department of Computer Engineering
Punjabi University Patiala (Pb.)

Navroz Kaur
Department of Computer Engineering
Punjabi University Patiala (Pb.)

ABSTRACT

The Wireless Sensor Network technology is a improved method of collecting the high sensitive information. In this paper discussion on various security methods is considered related to WSN. This paper is describing the fundamentals of secure data aggregation in WSN, identification of important parameters for the classification of secure data aggregation techniques in WSN, key characteristics of existing secure data aggregation techniques as well as comparing the existing secure data aggregation techniques with previous techniques. Instead of this introducing table of comparison based on various parameters such as security principles, prevention of attacks by protocols, aggregation function. In addition to this cryptographic techniques which are used to secure data in WSN.

KEYWORDS

Wireless sensor network, centralized server, attacks in WSN, black node detection , encryption techniques, security methods .

1 INTODUCTION

1.1 Definition: The wireless sensor network (WSN) is a sensor network consisting of sensor nodes which are spatially dispersed and dedicated autonomous. The function of these nodes is to monitor physical and environmental conditions of different places of the world. The most common parameters such as pressure, light, wind direction, speed of wind, intensity, sound, vibration, humidity, vital body functions , temperature as well as pollution level are monitored by sensor nodes.

1.2 Structure: wireless sensor network is a one kind of wireless network consisting various nodes called sensing nodes. These sensor nodes are tiny computers which work in the join form to make network. Also nodes are light in weight and portable. The most significant feature states that sensor nodes consists radio transceiver , a battery as well as a microcontroller which can be easily located as an energy resource externally. The function of the radio transceiver is to connect the sensor nodes or neighbor nodes with an external link while the microcontroller is an electronic circuit that plays a significant role to interface the sensor nodes thereby forming a complete circuit to effectively process, store, receive and send data to the base station.

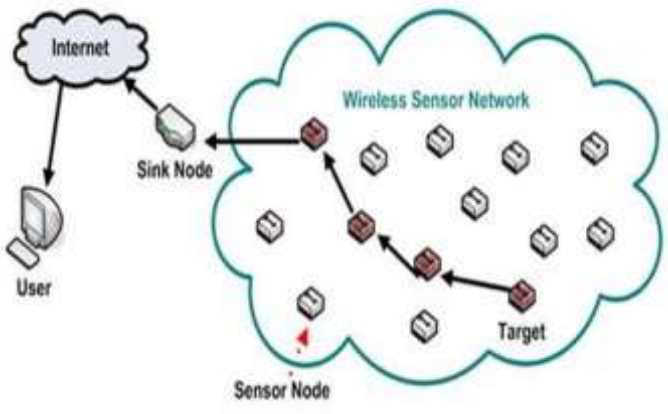

Figure 1: Structure of WSN

1.3 Applications: There are numerous applications of WSN like in industrial automation, traffic monitoring as well as control, medical device monitoring and so many other areas. Some of them are following:

- Disaster relief operation
- Military applications
- Environmental applications
- Medical applications
- Home applications

1.4 Complexity of WSN: The nodes of the WSN are work under number of constraints, for instance energy resource comprises supply of energy to transmit the data in a highly unspecified environment. Besides this data packets can be loss only due to unwanted error. Sometimes node congestion can be high. It can be reiterated that sending secure data in WSN is not easy work. Due to presence of malicious node and some attacks it is difficult to send secure data or effective information to the base station because nodes has the ability to communicate closely in their environment.

1.5 ATTACKS IN WSN:

Wireless sensor networks are subjected to various attacks only because of its broadcast nature of transmission medium. All the nodes communicate in dangerous environment in which nodes are not physically protected. In this case attackers can device several security threats in network to make it unstable.

TAXONOMY OF ATTACKS:

1.5.1 Goal-oriented attacks: In WSN term data confidentiality means the role of attacks is to simply break the encryption model used in the WSN deployment. In this attacker passively monitors the traffic of node . After analyzing the information which is sensitive it gains the authentication information for further pass to other node.

1.5.2 Performer-oriented attacks: These types of attacks can be either internal or external. In internal attack, attacker node does not belong to wireless sensor network but it also have the direct access to all the network information which leads to degradation of performance of network but in external attacks attackers are known for eavesdropping on transmittance of data which easily transmit the fake data along the real node which will lead to denial of services.

1.5.3 Layered attacks: Attackers can gain access to transmission media, create radio interference , prevent from legitimate sensor nodes to communicate or launch denial of service attacks in link layer like layer jamming . In this attacker collides the packets during transmission, exhausting node's resource and create confusion.

1.6 Effective approach to WSN: To deal with above type of attacks in WSN, trust management system is considered to be the most effective and efficient method. Trust factor is a very important and useful accordingly support in the process of decision making means decides which node is authorized to communicate in network.

MOTIVATION FOR WORK

Although a huge amount of review work exists regarding the security of user credentials but after assaying the work the following pinpoints emerged:

1. Paper addresses the problem of exploration of accessible security algorithms in wireless sensor network.
2. Papers failed to implement secure user authentication framework so that no unauthorized user can join the network.
3. Most significant problem is the cost.

This paper is defined and organized as follows: section 2 describes the various state of the art authentication techniques and need of secure network in wireless sensor network. Section 3 presents the relevant research questions to be addressed, key research areas and various existing algorithms giving their methodology, contributions and research gaps.

Section 4 gives the conclusions and future work for further research.

2 LITERATURE SURVEY

A lot of researchers have worked in this field and provide fool proof algorithms to provide the security in the wireless sensor network but no one is successful to provide efficient method. Every researcher has some limitations in research work which are discussing in following section:.

1. TRUSTED NEIGHBORS BASED SECURED ROUTING ALGORITHM

Most previous schemes have not considered malicious nodes in the network. The network described in this paper contains black hole nodes and malicious node drop packets. Thus the arrival ratio of the data packet decreases. To improve it, this scheme was proposed. In this ,when the source nodes send one data packet to the destination an abstract information is also transmitted to the destination. Thus, if the malicious node in the backbone drop the data packets but the destination receives the information from the source node , the destination will know that the routing path in the backbone contains malicious nodes . it also reduce its evaluation of the trust in the nodes in the routing path. After several rounds of data packet transmission the nodes will communicate each other. If nodes has lower trust , node will be identified as a malicious node . Thus in the next round of data transmission this node will not be selected in the backbone and with it data packet arrival ratio will also improve. There is one drawback of this scheme is that it unable to calculate the occurring ratio of malicious node. [1]

1.1Efficient Trust Management Algorithm

In trusted neighbor based technique one problem is encountered that is the calculation of node communication time with other nodes. To overcome this problem simple and efficient algorithm is implemented. In this algorithm firstly the value of trusted node is calculated to find the malicious node with the help of packet forwarding factor. calculated the value of the trusted node and found the malicious node on the basis of packet forwarding factor. It also determined the consistency of clusters and lifespan of the network with only one limitation that is the multi hope communication which increase the overhead cost in WSN. [2]

2 .DATA AGGREGATION TECHNIQUES

After finding the malicious nodes in the network is not enough to provide security in the network. So to provide security in WSN various aggregation techniques were based on various parameters such as security principles, prevention of attacks by protocols, aggregation function, and cryptographic techniques but these were failed to judge the accuracy and energy consumption over network and also discussed various security loopholes in wireless sensor network. [3]

2.1 Trusted And Reputation Model

The efficient and trusted model is proposed in WSN to determine the various effects of modes such as static, dynamic, oscillating to judge the accuracy, path length as well as energy consumption in network. Although it comprises various models like Eigen trust, bio- inspired, peer trust, linguistic fuzzy trust as well as reputation but it do not cover all major types of threats arise in WSN. [4]

2.2 Collaborative Lightweight Method

In WSN minimal overhead in regard to memory and energy consumption is also introduced. For this a collaborative lightweight method is designed in which works on a threshold value. For instance counselor tracked and send the warning information to that node whose trust fell below a warning threshold. After that the warning message warned the sensor node to check the black node and then sensor node modify the packet forwarding behavior to improve its relation with neighbor node. The limitation of this method is that the all nodes has the same name due to that one node is not reuse for some other. [6]

3.ATTACKS PREVENTING METHOD Unlike traditional networks ,the WSNs are very vulnerable to internal attacks from compromised nodes .

3.1 BETA BASED TRUSTED SCHEME

To improve the WSNs' information security as well as to minimize the probability of attacks the efficient technique is used called beta based trust and reputation method. In this research, the only limitation is that researchers failed to consuming energy in WSN optimal manner.[5]

3.2 IMPROVED TRUST MANAGEMENT SYSTEM

Above mentioned all the techniques did not specified the relation between nodes, only successful to find the malicious nodes in the network so for this a improved trust management system is proposed which is used to specify the relationship between nodes and also enhancing the utilization efficiency of that information which is coming from other node but the only limitation is that it fails to consuming energy in WSN in optimal manner.[7]

4. Distributed Energy Aware Trust Management method

One more thing is needed to be taken in mind that is the speed. Speed play an important role in WSN to detect the malicious nodes as soon as. To implement this method a distributed energy aware system is proposed in WSN which is routing based method. Its main aim to detect the set of attacks very quickly and also introduced the idea of energy awareness. [8]

5. NETWORK IMPROVEMENT BASED METHOD

The two-tiered network architecture of WSN is also designed for increasing network capacity and scalability, reducing system management complexity, and prolonging network lifetime. The limitation of their research they implement Authentication scheme at one level factor.[9]

6.INTERNET BASED SCHEMES As the Internet market grows, the importance of the WSN which is the network environment on which the Internet is based, is becoming more important.

6.1 PAIRED BASED KEY DISTRIBUTION

Using WSN, many sensor nodes can easily detect, store, process, and integrate object and environment information through gateways and send them wirelessly. But the main problem is their proposed method is more complex which deflate available energy of nodes highly. [10]

6.2 SECURE FRAMEWORK USING ECC

Above mentioned technique is unable to introduce a reliability and improved level of security .Despite of this technique a new technology, which permit a communications infrastructure for monitoring and tracking. It creating a major challenge for administrators in providing a good quality of service or in ensuring a good level of security, especially the security of data transmitted via the network. It also fails to manage the threats because it is not more robust.[11]

6.3 CRYPTANALYSIS MULTIGATEWAY IN WSN

WSN has some vulnerability because of its openness. For this reason, many researchers have proposed various user authentication schemes for added security of wireless sensor networks. Recently, Wu et al. proposed an authentication scheme for multi-gateway wireless sensor networks in Internet of Things deployment. Wu et al. claimed that their scheme is secure against user forgery attack and session key leakage but this Scheme cannot guarantee the security of authentication.[12]

7 COST REDUCTION METHOD FOR WSN It is very hard to reduce cost as well as to maintain staff intensity. Furthermore, remote meter reading is also accomplished through WSN. In this abstract the corresponding credits are transmitted over the WSN (Wireless Sensor

Network) to the client terminal to recharge on the ESAM and the related data are uploaded to the upper management centre, this way, avoiding the problem brought by IC card as the information carrier and reducing operating costs and staff labor intensity.[13]

7.1 ZIGBEE SHORT RANGE METHOD

Zigbee short-range wireless transmission technologies used which uses IEEE802.15.4 standard, features include low-power, low-rate, low-cost ... and so on. But ZigBee is applied to a considerable number of occasions. Consumers with a variety of physical sensors and home equipment, set up a smart home energy management system to handle a variety of situations that may occur at home.[14]

8. OTHER TECHNIQUES

In further research Wireless body sensor networks (WBSNs) have been utilized to acquire physiological signals such as electrocardiogram (ECG), photo plethysmogram(PPG),and electromyography (EMG) [1-8]. These signals as well as the features extracted from them should be properly protected to ensure the integrity and confidentiality of the data among others [9-11]. Compared with the traditional computer systems (TCSs), WBSNs only can provide a limited computation as well as low power capability. Thus the security methods on TCSs cannot be directly applied to WBSNs because they are too complex and require more computation ability and power resources [12].

8.1 WBANS

After that the WBANs enhance the efficiency of healthcare since a patient does not need to visit the hospital frequently. This characteristic is especially favorable for countries that are lack of medical staffs and medical infrastructure. In addition, the clinical diagnosis and emergency medical response can be realized by using the WBANs. [15]

8.2 DAG' S IMPLEMENTATION

Furthermore data provenance becomes indispensable when working in a distributed environment to gauge quality of data. To achieve adequate level of trust on provenance data, security of data provenance is equally important as provenance generation and dissemination. Provenance data is different from traditional data as provenance contains information about the entities and their relationships. Provenance data maintains DAG structure, where data keeps changing while the lineage information remains same.[16]

Table 1 Existing Algorithms for Secure node authentication

Author	Technique	Research gap
Monia Sukhchandan Randhawa and Sushma Jain	An Efficient Trust Management Algorithm	The Limitation of this research work is that it fails to handle the multi hop communication which leads to excessive cost in WSN.
Mukesh kumar and Kamlesh Dutta	Various Data Aggregation Techniques in Wireless Sensor Networks	Various security loopholes in wireless sensor network
Surinder Singh, Vinod Kumar	Evaluation of models over static, dynamic and oscillating modes which are trusted based.	Fails to cover all major types of threats arise in WSN

Chuanlei Zhang, Weidong Fang, Shi Qing Zhao	Beta based reputation and trusted evaluation system	Energy consuming problem in WSN in optimal manner.
X. Anita, J. Martin Leo Manickam	Collaborative Lightweight Trust (CLT) Management method for WSN	Specify the same name to all nodes which is the major difficulty in node communication
Yun Liu, Chen Xu Liu , Qing An Zeng	Secure data aggregation with improved trust management system in wireless sensor networks	consuming energy in WSN in optimal manner.
Yannis Slelios, Nikos, Sotiris Maniatis, HelenC leligou	Routing based distributed trust management system in WSN.	They do not cover indirect trust information of neighbor node to check the reliability of node.
Usha Jain, Muzzammil Hussain1 Dept. of Computer Science and Engineering, Central University of Rajasthan, Ajmer,	Simple Secure and Dynamic protocol for Mutual Authentication of nodes in Wireless sensor network.	They do not cover black whole attack properly in their research.

Manik Lal Das Dhirubhai Ambani	Efficient User Authentication and Secure Data Transmission in wireless sensor network	In their Research they do not cover Denial of service Attack , Compromise attack in WSN.
Rong Fan, Ling-Di Ping, Jian-Qing Fu, Xue-Zeng	A secure and Efficient User Authentication protocol for two tired wireless sensor network	The limitation of their research they implement Authentication scheme at one level factor.
Gun-Wook Choi	A Key Distribution system for user Authentication using pairing based in WSN	Their proposed method is more complex which deflate available energy of nodes highly.
Karim ZKIK Ghizlane ORHANOU Said EL HAJJI	A New Secure Framework in WSN using ECC Medical applications.	Their Framework is not more robust for manage the threats in WSN
Taeui Song, Jaewook Jung, Dongwoo Kang, Hyoungshick Kim and Dongho Won	Cryptanalysis of an Authentication Scheme for Multi Gateway Wireless Sensor Network	The limitation in their research work is their Scheme cannot guarantee the security of authentication

3. REVIEW METHOD

3.1 RESEARCH QUESTIONS

Research questions are the fundamental building blocks for scientist in order to plan and conduct any research; therefore it is compulsory to formulate such questions. Key questions encountered during my study are as follows:

- What are the existing techniques and algorithms for secure node authentication along with the research gaps in the existing literature?
- What are the key areas of research in the field of secure node authentication in WSN?

3.2 KEY RESEARCH AREAS

Wireless sensor networks have attracted a lot of interest over the last decade in wireless and mobile computing research community. Applications of WSNs are numerous and growing which range from indoor deployment scenarios in the home and the office to outdoor deployment in adversary's territory in a tactical battleground.

WSN became ubiquitous as they play a pivotal role in monitoring critical parameters of the environment pertaining to civilian and military applications. Sensors can also be embedded into wearable devices to track vital signs of patients in healthcare domain.

WSN is widely used in military applications such as military command, control systems, communications, computers, intelligence and surveillance systems. Some military applications are force tracking, battlefield, surveillance, targeting, battle damage assessment; also in chemical , biological , radiological and nuclear detection. Some environmental applications of sensor networks include tracking of movement of species that effect the livestock, irrigation, micro instrument for large scale earth monitoring and planetary exploration.

4. CONCLUSION AND FUTURE SCOPE

There is a need for effective security mechanisms in wireless sensor networks. The paper describes constraints, goals, obstacles, and security breaches based on different protocol layers, defensive measures, and security mechanism for wireless sensor networks.

5. REFERENCES

1. Geetha D. Devanagavi, N. Nalini 2014 .Trusted Neighbors Based Secured Routing Scheme Using Agents. Springer transactions on routing algorithm,014-1704-4.

2. Monia , Sushma Jain ,Sukhchandan randhava 2016. An Efficient Trust Management Algorithm in Wireless Sensor Network .Springer 0287-8_26.

3. Mukesh Kumar and Kamlesh Dutta 2009 .A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks. Springer India . 2009-1_1.

4. Vinod Kumar, Surinder Singh, N.P. Pathak 2015. Various trusted and reputation models wireless sensor networks. Springer Science ,1144-4.

5.Weidong Fang , Chuanlei Zhang , Shi Qing Zhao 2015. Evaluation system and reputation Beta-based Trust in WSN 1084-8045 Published by Elsevier Ltd.

6. X Anita , M.A. Bhagyaveni 2014. Collaborative Lightweight Trust Management Scheme. Published in Springer Science ,014-1998-2

7. Yun Liu, Qing-An Zeng 2015.Improved trust management scheme for secure data aggregation .Springer publications 015-0078-6

8. Yannis Stelios, Sitiris Maniatis, Helen C. Leligou 2009.Routing based Distributed Energy-Aware Trust Management System in Wireless Sensor Networks. Institute for Computer Sciences and Telecommunication 85-92.

9.Rong Fan, Ling-Di Ping, Jian-Qing Fu 2010, Xue-Zeng. Two tired architecture of WSN. Pan

College of Computer Science and Technology Zhejiang University 5626600

10.Gun-Wook Choi 2017. paired base key distribution scheme in wireless sensor network.IEEE publication 10.1109

11.Karim ZKIK Ghizlane ORHANOU Said EL HAJJI 2017. Secure framework using ECC

10.1109/ICEngTechnol.2017.8308144

12.Taeui Song1, Jaewook Jung2, Dongwoo Kang2, Hyoungshick Kim3 and Dongho Won4 2017.The Twelfth International Conference on Digital Information Management (ICDIM 2017) 6414-4

13.Qipeng Ma, Chenxu Duan, Xudong Ding, Tingwei Qian, Peiyong Duan Shandong Engineering Shandong Jianzhu University Jinan 2012. A design of Network Prepayment Meter Reading System based on Embedded Secure Access Module (ESAM) is presented in this paper 10.1109. IEEE International Conference .

14 Jui –Ho Chen ,Wen – Tsai Sung and Guo –Yan Lin 2017. Zigbee short range wireless transmission technologies ,the use of standard IEEE 802.15.4

15.Guanghe Zhang, Oluwarotimi Williams Samuel, Fanghua Liu, Shixiong Chen, Hui Zhou, Haoshi Zhang, and Guanglin Li 2017.Wireless body sensor networks (WBSNs) provide a platform to track and monitor human health status. 10.1109/EMBS.

16.Idrees Ahmed ∗, Abid Khan†, Muhammad Saleem Khan ‡, Mansoor Ahmed§ 2016. Provenance data maintains using DAG structure. Department of Computer Science COMSATS Institute of Information Technology. 2324-9013/TrustCom/BigDataS

17.Haneef, M.; Deng, Z. Design challenges and comparative analysis of cluster based routing protocols used in wireless sensor networks for improving network life time. Adv. Inf. Sci. Serv. Sci. 2012, 4, 450–459.

18. Harneet kaur 2010, “Energy Efficient Scheme for Clustering Protocol Prolonging the Lifetime of Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887) Volume 6– No.2, pp. 31-36.

19. Chandrakasan, A.P, Balakrishnan, Han application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. 2002, 1, 660–670.

20.Intanagonwiwat, C.; Govindan, R.; Estrin, D.; Heidemann, J. Directed diffusion for wireless sensor networking. IEEE/ACM Trans. Netw. 2003, 11, 2–16.

21. https://en.wikipedia.org/authen_node

22.Quantitative research https://en.wikipedia.org/wiki/quantitative_sreasearch