IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

Node Attestation for Reliable Communication in WSN

Ranjeet Kaur[1]* and Khushboo Bansal[2]

[1]Desh Bhagat University Punjab,India

[2] Desh Bhagat University Punjab,India

Available online at: www.ijcseonline.org

Received: Mar/23/2016 Revised: Apr /03/2016 Accepted: Apr/19/2016 Published: Apr/30/2016

***Abstract*— The wireless sensor network (WSN) is a mix of sensing, computation, and communication into a solitary small gadget. A sensor system comprises of a variety of various sensor systems of differing sorts interconnected by a wireless communication network. Sensor information is shared between these sensor nodes and utilized as data to a circulated estimation framework. The framework extricates important data from the accessible data. In this paper represent briefly various attacks and approaches to used for WSN.**

***Keywords*— WSN, attestation algorithm, routing strategy.**

I. INTRODUCTION

1.1 Wireless sensor network: A wireless sensor network is a wire and wireless system, which comprises of a few sensor nodes, sent in a specific field. A sensor node ought to have calculation, detecting and remote correspondence capacities. A wireless sensor network confines the radio recurrence channel, because of that is to say, precarious connections, breaking point of physical assurance of every sensor node real of every nodes association, variety topology what's more risk about directing security is high by movement spite nodes. A sensor network has constrained figuring and correspondence assets [1]. To defeat this obstruction, cooperation with encompassing nodes is required. As it were, data sharing between chains of importance is required as opposed to a various leveled approach.

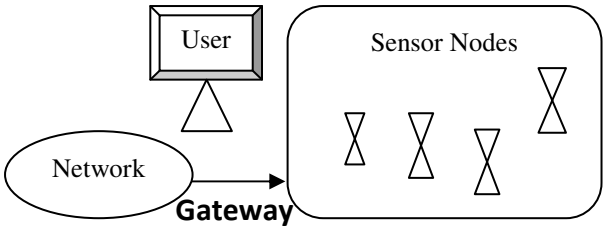

Fig 1.1: Wireless sensor network

A sensor network for the most part comprises of countless nodes for definite sensing and extendibility of sensing zones [2]. Subsequently, aggressors can undoubtedly catch sensor nodes and the attacker can attack the sensor node itself and the sensor network through a changed attack on the sensor node. In this way, the security of a sensor network is imperative. Sensor networks are connected to different fields running from extraordinary application fields, for example, wild environment observing, mechanical machine estimation and military reason estimation to day by day application fields, for example, fire checks and pollution observing.

1.2 Attacks in wireless networks: There are many attacks in WSN, some known attacks (intensively discussed in the references) that pose a significant threat to group communications over wireless networks and categorize these attacks based on their impacts, including data integrity and confidentiality, power consumption, routing, identity, privacy, and service availability [3].

1.2.1 Denial of Service Attack: Denial of Service attack is an endeavor to make a system inaccessible for its honest to goodness clients. An attacker messes around with information before it is perused by sensor nodes, in this manner bringing about false readings and in the long run prompting a wrong choice. A DoS attack for the most part targets physical layer applications in a situation where sensor nodes are found [4].

1.2.2 Node Capture Attack: In Node Capture Attack an aggressor physically catches sensor nodes and bargains they so that sensor readings detected by traded off nodes are off base or controlled. The attacker might likewise endeavor to concentrate key cryptographic keys like a gathering key from remote nodes that are utilized to secure interchanges in many wireless networks [5].

1.2.3 Eavesdropping attack: Eavesdropping is the procedure of social event data from a system by snooping on transmitted information and to listen stealthily is to furtively catch a private discussion over a classified correspondence in an unapproved way. The data continues as before yet its security is bargained. An aggressor listens stealthily furtively between any two nodes and might gather

the essential data viewing association, for example, MAC address and cryptographic data [6].

1.2.4 Collision Attack: In crash attack, attacker tries to degenerate the octet of transmitted packets. In the event that attacker succeeds in doing then at the less than desirable end the packets will be tossed because of checksum confuse. The retransmission of parcels could bring about depletion of fundamental assets i.e. energy of the sensor nodes [7].

1.2.5 Sybil attacks: A solitary nodes presents itself to different nodes with various parodied distinguishing pieces of proof (either MAC or system addresses). The attacker can imitate different nodes characters or just make various discretionary personalities in the MAC and/or system layer. At that point the attack postures dangers to other convention layers for samples, parcels navigated on a course comprising of fake characters are specifically dropped or changed an edge construct signature component that depends with respect to a predetermined number of nodes is ruined [8].

1.3 Unique Features of Sensor Networks: It ought to be noticed that sensor systems do offer a few shared traits with general specially appointed systems. Along these lines, protocol plan for sensor network must record for the properties of specially appointed network, including the accompanying. The lifetime requirements are forced by the constrained energy supplies of the nodes in the system. That forces temperamental correspondence because of the remote medium. There is requirement for self-setup, requiring almost no human mediation. Notwithstanding, a few extraordinary components exist in wireless sensor organizes that don't exist when all is said in done specially appointed networks. These elements show new difficulties and require change of outlines for traditional ad hoc networks [9].

1.3.1 Network Protocols: When outlining network protocol for wireless sensor networks, a few components ought to be considered. Above all else, due to the rare vitality assets, directing choices ought to be guided by some familiarity with the energy resources in the network. Besides, sensor networks are extraordinary from general specially appointed systems in that correspondence channels frequently exist in the middle of occasions and sinks, as opposed to between individual source nodes and sinks. The sink nodes are commonly more keen on a general portrayal of nature, as opposed to express readings from the individual sensor gadgets. In this way, correspondence in sensor networks is normally alluded to as information driven, instead of location driven, and data might be amassed locally as opposed to having every crude dat sent to the sinks. These one of a kind components of sensor systems have suggestions in the system layer and subsequently require a reexamining of protocol for data steering. Moreover, sensors frequently know about their own area to seriously evaluate their data. This area data can be used in the system layer for directing purposes. At last, if a sensor network is all around associated (i.e., superior to is required to give correspondence ways), topology control administrations ought to be utilized as a part of conjunction with the ordinary steering protocol. This segment depicts a percentage of the work that has been done to address these sensor network particular issues in the steering layer [10].

1.3.2 Resource-Aware Routing

As assets are to a great degree constrained in remote sensor networks, it is critical to consider how to most effectively utilize them at all levels of the protocol stack. A wide range of methodologies have been created that consider the sensors' resources when settling on directing choices. At first, conventions were produced that considered just the sensors' energy assets. Later work considered individual sensors' energy as well as the sensors' detecting assets [11].

1.3.3 Data-Centric Routing Protocols

Sensor systems are on a very basic level unique in relation to specially appointed systems in the information they convey. While in specially appointed systems singular information things are imperative, in sensor network it is the total information or the data conveyed in the information instead of the genuine information itself that is critical [12]. This has prompted another worldview for systems administration these sorts of gadgets – information driven steering. In information driven steering, the end nodes, the sensors themselves, are less imperative than the information itself. In this manner, inquiries are postured for particular information instead of for information from a specific sensor, and steering is performed utilizing learning that it is the total information as opposed to any individual information thing that is imperative [13].

1.3.4 Geographic Routing

Some of the time the remote sensor network requires an inquiry packet to be sent to a specific area of enthusiasm for the system. A characteristic way to deal with perform this sending is to use geographic sending [14]. Geographic sending diminishes the measure of steering overhead, which is to a great extent because of course disclosure, and requires little memory usage for course reserving contrasted with common location driven impromptu directing protocols. Besides, geographic directing protocols can empower geologically circulated information stockpiling systems, for example, Geographic Hash Tables [15].

2 REVIEW OF LITERATURE

Doo Seop Yun et al [1] "A study on the vehicular wireless base-station for in-vehicle wireless sensor network system" In this paper, we study on the vehicular wireless base station for in-vehicle wireless sensor network system. We introduce in-vehicle wireless sensor network system

applying wireless sensor network technologies. The in-vehicle wireless sensor network system greatly consists of the vehicular wireless base-station, vehicular wireless sensor nodes, and wireless OBD (On-Board Diagnostics) module. Here, we describe the vehicular wireless base-station as sub-system of in-vehicle wireless sensor network system. The vehicular wireless base-station carries out roles which process ECU (Electronics Control Unit) information obtained from wireless OBD module and sensor information received from a number of vehicular wireless sensor nodes.

Tseng-Yi Chen et al [2] "An Efficient Routing Algorithm to Optimize the Lifetime of Sensor Network Using Wireless Charging Vehicle" Although wireless sensor devices usually have limited power, they are widely deployed in various applications, such as in remote sensing for forestry applications, military monitoring, and animal behavior. Most sensor applications deploy sensor devices in natural environments, such as forests, tunnels, and caves, to monitor targets and to collect data. To permanently monitor target environments, the battery in a sensor device needs to be recharged as its battery capacity the limited. A wireless charging vehicle uses wireless charging technology to prolong the lifetime of sensor network applications by recharging the device's battery. The wireless charging vehicle is usually equipped with a large capacity battery, an electromagnetic field, and wheels such that it can move throughout an entire sensor network to charge sensors' batteries. When the wireless charging vehicle does not need to recharge any sensor's battery, it stays at a service station to recharge its own battery. Hence, a wireless charging vehicle needs to consider two things: sensor network lifetime, and vehicle energy consumption. This work proposes a geometric solution called the Dynamic Path Generation Scheme (DPG-Scheme) to arrange the Wireless Charging Vehicle's (WCV's) travelling path while minimizing a vehicle's energy consumption and maximizing a sensor network's lifetime.

Mitra, S. et al [3] "Energy aware fault tolerant framework in Wireless Sensor Network" Wireless Sensor Network, composed of tiny sensor devices and wireless network, is mainly responsible for any kind of ambience surveillance. Due to the peripheral atmosphere in which it is deployed, tiny sensors or the network might be too much fault prone. It is beneficial if and only if sensed values are fault free and it can traverse through fault free path. Thus it is necessary to monitor the network and the sensor nodes in regular interval to generate required result for application specific decision making. Network lifetime play the crucial role in order to monitor network health. It is critical as a certain percentage of the total number of sensor nodes along with its connectivity should remain alive for smooth operation of the network. The objective of this paper is to propose an energy aware fault tolerant framework in wireless sensor network. Fault detection algorithm and maximization of network lifetime in wireless sensor network is also proposed together with the calculated energy consumption of the sensor nodes for performing various tasks, including self fault checking, in the network. Simulation result for the proposed algorithm is also presented in this paper.

Deshpande, P. et al [4] "Techniques improving throughput of wireless sensor network: A survey" In wireless sensor networks, maintaining the higher throughput is the main concern. Wireless senor networks are basically formed with a few powerful base stations and a large number of resource-constrained sensor nodes. The wireless sensor network composed of n number of sensors or nodes, where each and every node is connected to one or several nodes or sensors. For providing low data rate for short coverage and long battery life, zig bee is used in wireless sensors network and ultimately zig bee nodes are used in wireless sensor network which are called as zig bee sensor nodes. Wireless sensor nodes of zig bee system basically build on two aspects of protocol stack that are IEEE 802.15.4 standard and zig bee protocol. The problem that sensors usually face in wireless sensor network is that when data packets are transferred from one node to another node, the throughput of the wireless sensor network decreases because of packet collisions and high network traffic. In order to overcome this problem, various methods have been discussed to improve the throughput.

Makhdoom, i. Et al [5] "a novel code attestation scheme against sybil attack in wireless sensor networks" wireless sensor networks (wsn) due to their distributed nature are vulnerable to various external and insider attacks. Classic cryptographic measures to protect against external attacks to some extent but they fail to defend against insider attacks involving node compromise. A compromised node can be used to launch various attacks of which sybil attack is the most prominent. In this paper we carry out a detailed review and analysis of various defenses proposed against sybil attack. We identify their strengths and weaknesses and also propose a novel one way code attestation protocol (owcap) for wireless sensors networks, which is an economical and a secure code attestation scheme that protects not only against sybil attack but also against majority of the insider attacks.

3 APPROACHES USED

3.1 TPM-Based Attestation: Existing attestation protocols are based on the TPM's ability to report the system configuration to a remote party. The complete system configuration, as denoted in the PCRs of the attesting entity, must be transmitted to the verifying entity. The verifying entity evaluates the trustworthiness of the attested entity by comparing the received SML and PCR values with given reference values. Since the verifying entity receives the current platform configuration directly, we refer to this as explicit attestation. However, in hybrid WSNs most sensor nodes do not possess enough resources to perform public key cryptography and the transmission of large messages increases the energy consumption significantly. This causes explicit attestation to be inapplicable in WSNs. To perform an attestation in WSNs, computation intensive operations must be transferred to nodes which posse's sufficient computational power and resource constrained sensor nodes need only to perform minimal verification computations. The sealing concept of the TPM enables an attestation without directly transferring the platform configuration (PCR values and SML values). We refer to this as implicit attestation. This approach minimizes the amount of transmitted data and does not require public key cryptography on resource constrained nodes. Sealing provides the functionality to bind data to a certain platform configuration. Our protocols smartly exploit this property to enable a lightweight attestation of the trustworthiness of the attested entity.

3.2 Software-Based Attestation: The main disadvantage of TPM-based attestation is that the platform configuration only reflects the initial load-time configuration. Therefore, memory modifications during the runtime cannot be detected, e.g., buffer-overflows. To overcome this shortcoming, attestation software may measure the memory and report the values to a remote party. In this case, the attestation software forms the trust anchor which must be protected against tampering. In approaches based on measuring the execution time of an optimal attestation routine is introduced. The routine cannot be optimized further, i.e. the execution time cannot be made faster which prevents an adversary from injecting malicious code without detection. However, the success of this approach relies critically on the optimality of the attestation routine and on minimal time fluctuations of the expected responses. Particularly in WSNs with multichip verification and external influences, time intervals for responses can vary. In these cases the attestation would fail, even though a sensor node is in a trustworthy system state.

3.3 Noise Filling Techniques: For memory filling we focus on the program memory of the sensor node rather than data memory space since data memory space is much smaller than program memory space. That means the amount of available space for the attacker in data memory is assumed not large enough to put original code. Depending on WSN applications, we propose two filling approaches to achieve the goal of filling the free memory space with random noise known to the attester. The memory should be after filling, although filling the empty memory of sensor node with incompressible random noise by attester before the deployment is simple and effective, this is not applicable for all WSN applications. Thus, for filling the sensor's memory after the deployment, a post-deployment noise filling technique is proposed.

4. CONCLUSION

Wireless sensor network is used to send the information for the different fields such as environment monitoring, industrial machine measurement and military purpose measurement to daily observed fields such as fire monitoring and pollution monitoring. In the wireless network a number of sensor nodes are available for sensing the information from wide area network. In the network various nodes have to be provided their integrity to collect the information because attacker can be easily performing attacks by capturing information of sensor nodes so attacker can easily perform attack on the sensor nodes or on the network by modifying attacking strategy. In this paper, wireless sensor network, its attacks and approaches are briefly discussed. The scope of wireless sensor network is to find wide range of usability and functionality. So, a secure network technique can take this technology to the heights.

REFRENCES

[1] Satish Kumar, "*A Study of Wireless Sensor Networks-A Review*", International Journal of Computer Sciences and Engineering, Volume-04, Issue-03, Page No (23-27), Mar -2016, E-ISSN: 2347-2693.

[2] AbuHmed, T "*Software-Based Remote Code Attestation in Wireless Sensor Network*" IEEE Conference on Global Telecommunications Conference, pp- 1 – 8, 2009.

[3] Dazhi Zhang "*DataGuard: Dynamic data attestation in wireless sensor networks*" IEEE Conference on Dependable Systems and Networks (DSN), pp. 261 – 270, June 28 2010-July 1 2010.

[4] Yong-Sik Choi "*A study on sensor nodes attestation protocol in a Wireless Sensor Network*" IEEE Conference on Advanced Communication Technology (ICACT), pp. 574 – 579, 7-10 Feb. 2010.

[5] Rohit Aggarwal and Khushboo Bansal , "*An Efficient Intruder Detection System against Sinkhole Attack in Wireless Sensor Networks: A Review*", International Journal of Computer Sciences and Engineering,

Volume-04, Issue-04, Page No (64-68), Apr -2016, E-ISSN: 2347-2693

[6] Singh, Umesh Kumar, et al. "*An Overview and Study of Security Issues & Challenges in Mobile Ad-hoc Networks (MANET)*" International Journal of Computer Science and Information Security, Vol-9 (4), (2011): 106-111.

[7] I.. R. Chen "*Reliability Analysis of Wireless Sensor Networks with Distributed Code Attestation*" IEEE Conference on IEEE Communications Letters, pp. 1640 – 1643, 2012.

[8] Doo Seop Yun "*A study on the vehicular wireless base-station for in-vehicle wireless sensor network system*" IEEE Conference on Information and Communication Technology Convergence (ICTC), pp- 609 – 610, 2014.

[9] Tseng-Yi Chen "*An Efficient Routing Algorithm to Optimize the Lifetime of Sensor Network Using Wireless Charging Vehicle*" IEEE Conference on Mobile Ad Hoc and Sensor Systems (MASS),pp- 501 – 502, 2014.

[10] Mitra, S "*Energy aware fault tolerant framework in Wireless Sensor Network*" IEEE Conference on Applications and Innovations in Mobile Computing (AIMoC), pp- 139 – 145, 2014.

[11] Makhdoom, I. "*A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks*" IEEE Conference on Software Engineering Conference (NSEC) ,pp- 1 – 6, 2014.

[12] R.Nathiya and S.G.Santhi, "*Energy Efficient Routing with Mobile Collector in Wireless Sensor Networks (WSNs)*", International Journal of Computer Sciences and Engineering, Volume-02, Issue-02, Page No (36-43), Feb -2014, E-ISSN: 2347-2693

[13] Vinolia A, Jagajothi G, "*Estimating Localization for intruder detection in WSN*", International Journal of Computer Sciences and Engineering, Volume-02, Issue-06, Page No (33-38), Jun -2014, E-ISSN: 2347-2693

[14] Makhdoom, I "*A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks*" IEEE Conference on Software Engineering Conference (NSEC), 2014, pp- 1 – 6.

[15] Deshpande, P. "*Techniques improving throughput of wireless sensor network: A survey*" IEEE Conference on Circuit, Power and Computing Technologies (ICCPCT), pp- 1 – 5, 2015.

