A Review of User Authentication for Heterogeneous Wireless Sensor Network

Jasmine Kaur[1], Sukhwinder Sharma[2]
[1]*M.tech (student), Department of Computer Science, Baba Banda Singh Bahadur Engineering College, Fatehgarh*
[2]*Assistant Professor, Department of Computer Science, Baba Banda Singh Bahadur Engineering College, Fatehgarh*

Abstract **-** Wireless sensor networks have been investigated lengthily over the past few years. They were first used by the military for observation purpose and have since extended into industrial and civilian uses such as weather, pollution, traffic control, and health care. One characteristic of wireless sensor network on which research has been conducted is the security of wireless sensor networks. The concept of Internet of Things, which is already at our front doors, is that every entity in the Internet communications is interconnected into a global dynamic expanding network. Sensors and smart objects are next to classical compute devices key party of the IOT. We can already exploit the benefits of the IOT by using various wearable's or smart phones which are full of diverse sensors and actuators and are connected to second via GPRS or Wi-Fi. Because sensors are a key division of IOT, thus are wireless sensor networks. Researchers are already working on original techniques and resourceful approach on how to integrate WSN better into the IOT environment. Their scheme presented a novel advance anywhere a user as of the IOT can authenticate with a specific sensor node from the HWSN without having to converse with an opening node. Besides their proposal is highly efficient since it based on a simple symmetric cryptosystem. This paper focuses on overcoming the security weaknesses.

Keywords **-** Wireless Sensor Network, Security issues, Scheme internet of things, GPRS and encryption.

I. INTRODUCTION

A wireless sensor network (WSN) is consisting of spatially distributed autonomous devices using sensors to view physical or environmental conditions. WSN systems incorporate a gateway that provide wireless connectivity back to the wired world and distributed nodes. Wireless Sensor Network (WSN) is crucial for the future of Internet [1] of Things (IOT) since they cover a wide application range important for the IOT. They are a complex of small, wireless, ad hoc sensor nodes also called motes, which are consistent and deployed in an area of notice (e.g. home, forest, battle field, etc.). They are used in a wide range of claim scenarios, like armed healthcare, environment, home, etc. The sensors nodes are resource constrained and thus have a incomplete processing power, transmission range and battery life. Since WSNs are evermore attached to the IOT phenomenon, they in attendance new challenges and opportunities. Wireless sensor networks (WSNs) are rapidly growing in popularity due to the low cost solutions[2] for a variety of challenges in the real-world. WSN has no infrastructure support, is quickly deploy in a region with some low-cost sensor nodes, is employed for monitoring the environment, and is rigid to maintain its security. Multichip communication is preferred in WSN as the number of nodes is very large, and sensor nodes have constraint with admiration to power, computation, communication, and storage. Security in WSN becomes vital since the nodes after the operation cannot be manually maintained and observed. This situation becomes a main issue in WSN due to its system of communication. The authentication is provided to the data that can be sent or access by any node in the net. Also, it is critical to prevent and gain the information from the unauthorized users. As new intimidation and attack model are proposed, several kinds of authentication mechanisms have been introduced in WSN security.

II. AUTHENTICATION IN WIRELESS SENSOR NETWORK

In Wireless Sensor Networks Authentication is a process by which the individuality of a node in a network is established and guarantee that the data or the control messages originate from an authenticated source. Authentication mechanism can be differentiated based on the [3] following criteria:

- Authenticate uni-cast, multicast, or broadcast messages
- Shared key or asymmetric (public key) cryptographic method
- Static, mobile, or both aspects of WSN.

A variety of researches have focused on point-to-point authentication mechanism, which validate uni-cast messages in WSN. In spite of being secure, uni-cast methods cannot be applied straight to either multicast or broadcast messages. Broadcast messages are straight obtained from the reliable sources and cannot be changed during transmission [4]. The basic components of a broadcast authentication process are:

- Examination the source identity from which the message originate
- Confirm the message truthfulness for ensuring the message originality

Various authentication procedures consist of:-

- One-way authentication
- Two mode or mutual authentication
- Three mode authentication
- Contained authentication

III. ARCHITECTURE OF WIRELESS SENSOR NETWORK

A sensor node has to be capable of with the correct sensors, the necessary computation unit, memory resources, and adequate communication facilities to fulfil certain task. Usually, a sensor node is comprised of four basic components: one or additional sensor elements, a set (power unit), a memory and notebook unit, and a transceiver, as shown in Figure 1.1.

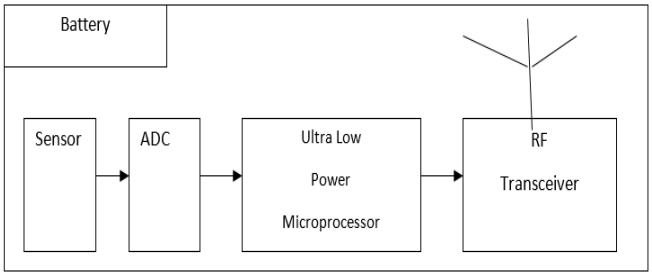

Fig.**Error! No text of specified style in document.**WSN Structure

A node may also have additional application-dependent components such as a position judgment system, assemble or a power generator. Sensing units are usually composed of sensors and analogue to digital converters (ADCs). The analogue signal shaped by the sensors (based on the observed phenomena) is converted to digital signal by the ADC. The rehabilitated signals are received by the processing unit. The processing unit, which is associated with a certain quantity of recollection, manages the node operational with others when executing the sensing task. Obtainable sensors in the market contain generic (flexible) nodes and entry (bridge) nodes. A generic (multi-purpose) sensor node's task is to take capacity from the monitor environment. Gateway (bridge) nodes gather data from generic sensors and relay them to the bottom station. Entrance nodes have higher processing capability, battery power, and [3] transmission (radio) series. A mixture of general and entrance nodes is typically deployed to form a WSN.

IV. SECURITY challenge IN WSN

- Data in confidence
- verification
- Availability
- Authorized
- Integrity
- Non-Repudiation

V. RELATED WORK

Sandra Sendra, Jaime Lloret, et al., 2011[4] Wireless networks have become increasingly popular due to their wide range of application. Energy utilization is one of the major constraints of the wireless sensor node and this restraint combined with a characteristic deployment of large number of nodes has added many challenges to the design and management of wireless antenna networks. They are analyze from several points of view: Tool hardware, broadcast, MAC and routing protocols. **Raghavendra V. Kulkarni, et al.,2010[5]** These papers outlines issue in WSNs introduce PSO and discusses its suitability for WSN application. It also presents a brief review of how PSO is tailored to address these issues. **Gogu, A. ; Lab. Heudiasyc, et al., 2011 [6]** The Wireless Sensor Networks (WSNs) design related questions give rise to new multifaceted and difficult hypothetical trouble and challenges in operations research and optimization area. As WSNs happen to more and more pervasive, a good understanding of these problems in terms of theoretical complexity is of great help in designing suitable algorithms. In this document, they look at some of the most fundamental optimization trouble associated to reporting, topology control, scheduling, routing and mobility in WSNs. Then they focus on their complication and analyze the differences that exist with the counterpart conventional theoretical problems or persons already studied in traditional networks. They present as they some of the main methods proposed in the literature and report some open issues regarding these problems. **Debmalya Bhattacharya1 and R.Krishnamoorthy, 2011[7]** Wireless Sensor Networks (WSNs) consist of a system of wireless nodes that have the ability to sense a constraint of interest. Sensors of different types are deployed all over and pervasively in varied environments such as office building, nature assets, battle fields, mobile networks, etc. The paper presents such a design which minimizes cost and power utilization, thus attractive the life time of the node. **Jun Luo and Liu Xiang,2011[8]** This paper focuses on exploiting mobility to improve the network lifetime of a WSN. They present a general optimization framework that is able to capture several aspects of maximizing network lifetime (MNL) involving movable entities. They also in attendance certain numerical results where engineering insights can be acquire.

VI. INSPIRATION

Communication between each node in a WSN (due to its inherent kind) distinguishes WSNs from previous wireless networks. Hence, many new protocols have been proposed for the communication exertion in WSNs. These protocols have to be designed with concern for these inherent features along with the function and architectural requirements. Therefore, the selection of a good set of protocols for a given task prior to a WSN's practical operation is an important issue [9].

With the proper set of protocols selected, the number of nodes deployed in a fixed area draws our deliberation. Typically, nodes compactness range from few sensor nodes to hundreds in a fixed area. When a great number of nodes are deploying, can users flattering utilize the high density nature of the WSN? Can they still maintain elementary

treatment in the objective area in the case that some nodes fail (Note that failure of some sensor nodes may not damage the overall routine of a WSN)? Normally, the design progression follow the order that persons in this ground firstly put more and more endeavour into inventing new protocols and new applications; then the answer are build, competent and evaluated either by reproduction or test beds; even sometimes an actual system has to be deployed so that researchers can learn by empirical evidence. A more scientific analysis procedure is ideally required before a WSN is practically deployed.

It is accepted that the current designers in the area are mainly experts in wireless sensor network and hardware who might perceive the communication behaviour between each nodes at the bit level. As WSNs immerse deeper into popular lives, they must start to include less particular users. In such cases, a scheme which can offer optimal solutions based on specialist information and can be easily used is powerfully preferred to support a wider audience of users [10].

VII. EXISTING PROBLEMS

Security in wireless sensor networks becomes crucial since the nodes after the operation cannot be manually maintained and experiential. These situations become a major issue in WSN due to its network of announcement. The verification [11] is provided to the data that can be sent or accessed by any node in the network. Also, it is significant to prevent and gain the in sequence from the unauthorized users. As new intimidation and attack models are planned, several kinds of authentication mechanisms have been introduced.

VIII. CONCLSUION

In current times, the technology of wireless sensor network has a great crash on technical fields like wireless message, information technology, and electrical etc. functionalities with a typical processor network as it is a special type of network. It also exhibit several kind that are unique to it. Though the major problem faced in this knowledge is that the sensor nodes run out of energy very quickly. Many routing protocols have been planned to solve this problem mainly focus on the success of minimizing the energy utilization in the sensor system. The authentication is provided to the data that can be sent or accessed by any node in the network. Also, it is significant to prevent and gain the information from the unauthorized users. As new threats and attack models are proposed, several kinds of authentication mechanisms have been introduced.

IX. REFERENCES

[1]. M. M. Chandane, S. G. Bhirud, S. V. Bonde, "Mobile Communication and Power Engineering Communications in Computer and Information Science Volume 296, pp 33-40, 2013.

[2]. Y. Sankarasubramaniam, I. E Akyildiz and S. W. Mchughli, "Energy Efficiency based Packet Size Optimization in Wireless Sensor Networks", IEEE, 2003.

[3]. Yuebin Bai, Shujuan Liu, Mo Sha2 Yang Lu, Cong Xu, "An Energy Optimization Protocol Based on Cross-Layer for Wireless Sensor Networks", IEEE, Vol.3, pp.27-33, 2008.

[4]. Sandra Sendra, Jaime Lloret, Miguel García and José F. Toledo, "Power saving and energy optimization techniques for Wireless Sensor Networks" IEEE, Vol.6 pp. 439-452, 2011.

[5]. Raghavendra V. Kulkarni, Senior Member, IEEE, and Ganesh Kumar Venayagamoorthy, Senior Member, "Particle Swarm Optimization in Wireless Sensor Networks: A Brief Survey"IEEE, 2010.

[6]. Gogu, A. ; Lab. Heudiasyc, Univ. de Technol. de Compiegne, Compiegne, France ; Nace, D. ; Dilo, A. ," Optimization Problems in Wireless Sensor Networks",IEEE, pp. 302-309 2011.

[7]. Debmalya Bhattacharya1 and R.Krishnamoorthy, " Power Optimization in Wireless Sensor Networks " IJCSI, Vol.8, pp.415-419,2011.

[8]. Jun Luo and Liu Xiang, "Prolong The Lifetime of Wireless Sensor Networks Through Mobility: A General Optimization Framework" IEEE, pp. 583-590,2011.

[9]. Patil, Shantala, et al. "A Survey on Authentication Techniques for Wireless Sensor Networks." International Journal of Applied Engineering Research7.11 (2012): 2012.

[10]. Farash, Mohammad Sabzinejad, et al. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment." Ad Hoc Networks 36 (2016): 152-176.

[11]. M. Ali and Z. A. Uzmi. An energy-e_cient node address naming scheme for wireless sensor networks. In IEEE International Networking and Communi- cations Conference (INCC'04), 2004