COMMUNICATION SECURITY OF WIRELESS NETWORK OF INTERNET BY INTERNET OF THINGS

Bahaedden mohamed kafu
Research Scholar
Alfa University

Abstract: The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. It has been known that WSNs are integrated into the "Internet of Things", where sensor nodes join the Internet dynamically, and use it to collaborate and accomplish their tasks. But if a wireless sensor network (WSN) is integrated into the Internet as a part of the Internet of things (IoT), there will appear new security challenges, such as setup of a secure channel between a sensor node and an Internet host. A number of already established schemes like SL, HWY and HOOSAC have been implemented in the past. Out of these, HOOSAC is the most secure scheme. But even after being a very secure scheme, the main limitation of this scheme is that it employs IBC (Identity based Cryptography) for the Wireless Sensor Network. Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key.

Keywords: IoT, Internet, Wireless Network, Security, Communication Network, Internet of Things

INTRODUCTION

A Wireless Sensor Network (WSN) consists of a large number of tiny wireless sensor nodes (often referred to as sensor nodes or, simply, nodes) that are, typically, densely deployed. Mobile communications and wireless networking technology has seen a thriving development in recent years. Driven by technological advancements as well as application demands various classes of communication networks have emerged such as Cellular networks, Ad hoc Networks, Sensor Networks and Mesh Networks. Cellular Networks are the infrastructure dependent networks. Ad hoc networks are defined as the category of wireless networks that utilize multi hop radio relaying since the nodes are dynamically and arbitrarily located. Ad hoc networks are infrastructure independent networks. A Wireless Sensor Network (WSN) is a collection of tiny devices capable of sensing, computation and wireless communication operating in a certain environment to monitor and control events of interest in a distributed manner and collectively react to critical situations. WSN applications span various domains such as environmental and building monitoring and surveillance, pollution monitoring, agriculture, health care, home-automation, energy management, earthquake and eruption monitoring. Notably, through collaboration WSNs can organize efficiently, prolong system lifetime, handle dynamics, detect and correct errors, all with the final goal of eventually executing reliably the user application.

Moreover, collaborative WSNs are integrated as basic elements of collaborative IoT technologies to create novel pervasive smart environments. This special session focuses on exploring collaborative techniques to make WSNs more reliable, intelligent, effective and easy-to-use in academic- and industry-related scenarios and to integrate them with IoT technology.

Nodes measure the ambient conditions in the environment surrounding them. These measurements are, then, transformed into signals that can be processed to reveal some characteristics about the phenomenon. The data collected is routed to special node, called sink node (also called Base Station) [1]. Then, typically, the sink node sends data to the user via Internet or satellite, through a gateway. Combining the advantages of wireless

communication with some computational capabilities, WSNs have an endless array of potential applications in both military and civilian applications, including robotic land-mine detection, battlefield surveillance, target tracking, environmental monitoring, wildfire detection, catastrophe monitoring, structural monitoring, security, industry, agriculture, home, traffic monitoring, for monitoring natural phenomena etc. [2].

Components of Wireless Networks

The important components of wireless sensor network are discussed below:

- **Sensor Node:** A sensor node is the core component of a WSN. Sensor nodes can take on multiple roles in a network, such as simple sensing; data storage, routing, and data processing.
- **Clusters:** Clusters are the organizational unit for WSNs. The dense nature of these networks requires the need for them to be broken down into clusters to simplify tasks such a communication [2].
- **Cluster heads:** Cluster heads are the organization leader of a cluster. They often are required to organize activities in the cluster. These tasks include but are not limited to data-aggregation and organizing the communication schedule of a cluster [3].
- **Base Station:** The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.
- **End User:** The data in a sensor network can be used for a wide-range of applications [1]. Therefore, a particular application may make use of the network data over the internet, using a PDA, or even a desktop computer.

Internet of Things (IoT)

The term 'Internet of Things' describes a number of technologies and research disciplines that will enable the Internet to reach out into the real world of physical objects. Technologies like RFID, short-range wireless communications, real-time localization, ad hoc and wireless sensor networks (WSNs) are now becoming increasingly common and all will take part in the Internet of Things (IOT). According to the IOT paradigm, physical objects will be equipped with some communication capabilities, which will be exploited to coordinate their action and in particular the way these objects influence the surrounding physical space. A common example is that of the books in a library, which could be equipped with RFID tags, so that each book could be precisely located by a WSN system deployed in the library. This information could then be fed to any search engine running on a computer located within the library or even outside (given that this computer has the right access credential for this data. This example could be easily extended to our houses or offices, so that it will be possible to acquire the physical location of objects within buildings through a dedicated WSN infrastructure connecting the physical world to the Internet domain. The complete realization of the above vision requires the solution of many technical challenges.

The expression "Internet of Things" was instituted by British business visionary Kevin Ashton in 1999 [9]. Typically, IoT is relied upon to offer propelled integration of gadgets, frameworks, and administrations that goes past machine-to-machine correspondences (M2M) and spreads a mixed bag of conventions, spaces, and applications.The interconnection of these implanted gadgets (counting shrewd articles), is required to introduce mechanization in almost all fields, while likewise empowering propelled applications like a Smart Grid [11] and extending to the regions, for example, Smart city.

Things, in the IoT, can allude to a wide assortment of gadgets, for example, heart checking inserts, biochip transponders on homestead creatures, electricmollusks in waterfront waters [14] vehicles with implicit sensors, or field operation gadgets that help fire-contenders in inquiry and rescue [15]. These gadgets gather valuable information with the assistance of different existing advancements and after that independently stream the information between other devices [16]. Current business samples incorporate brilliant indoor regulator frameworks and washer/dryers that use Wi-Fi for remote observing.

Other than the plenty of new application zones for Internet joined computerization to venture into, IoT is additionally anticipated that would create a lot of information from different areas that is totaled rapidly, in this manner expanding the need to better record.

Amid the previous couple of years, in the zone of remote interchanges and systems administration, anovel ideal model named the Internet of Things (IoT) which was initially presented byKevin Ashton in the year 1998, has picked up progressively more consideration in theacademia and industry. By inserting short-extend portable handsets into a widearray of extra devices and ordinary things, empowering new types of correspondence in the middle of individuals and things, and between things themselves, IoTwould add another measurement to the universe of data and communication. Unquestionably, the fundamental quality of the IoT vision is the high effect it will have on several parts of each day life and conduct of potential clients. From the perspective of a private client, the most clear impacts of the IoT will be noticeable in both working and household fields. In this setting, helped living, keen homes and offices-wellbeing, improved learning is just a couple of samples of conceivable application scenarios in which the new ideal model will assume a main part sooner rather than later. Similarly, from the point of view of business clients, the most evident outcomes will be equally obvious in fields, for example, robotization and modern assembling, logistics, business process administration, keen transportation of individuals and merchandise. Be that as it may, numerous testing issues still should be tended to and both technological as well as social bunches should be united before the vision of IoT turns into a reality. The focal issues are the means by which to accomplish full interoperability in the middle of interconnected devices, and how to furnish them with a high level of adroitness by empowering their adaptation and self-ruling conduct, while ensuring trust, security, and privacy of the clients and their information. All the more over, IoT will represent a few new problems concerning issues identified with proficient usage of assets in low-fuelled resource constrained items. A few mechanical, institutionalization and examination bodies are at present included in the activity of improvement of answers for satisfy the innovative necessities of IoT.The goal of this paper is to give the peruse a thorough talk on thecurrent best in class of IoT, with specific concentrate on what have been done in the Internet of Things zones of convention, calculation and framework configuration and improvement, and what are thefuture examination and innovation patterns. Whatever is left of the report is sorted out as takes after [3].

The Internet of Things (IoT) is a registering idea that depicts a future where every day physical articles will be joined with the Internet and will have the capacity to identifythemselves to different gadgets. The term is firmly related to RFID as the methodof correspondence, in spite of the fact that it could likewise incorporate other sensor advancements, otherwireless innovations, QR codes, etc. In the setting of "Web of Things" a "thing" could be characterized as a genuine/physical ordigital/virtual element that exists and move in space and time and is fit for being identified. Things are generally distinguished either by allocated recognizable proof numbers,names and/or area addresses.The Internet of Things infers a cooperative association among the genuine/physical, thedigital/virtual universes: physical elements have computerizedpartners and virtualrepresentation; things get to be connection mindful and they can sense, communicate,interact, trade, information, data and learning.

1.4.1 Vision for the IoT

In the examination groups, IoT has been characterized from different alternate points of view what's more, thus various definitions forIoT exist in the writing. The purpose behind obvious fluffiness of the definition originates from the way that it is grammatically made out of two terms - Internet and things. The first pushes towards a system situated vision of IoT, while the second has a tendency to move the attention on non-specific items. to be coordinated into a typical structure.However, the expressions "Web" and 'things', when assembled expect a significance which presents a troublesome level of advancement into the ICT world. In reality, IoT semantically implies an "overall system of interconnectedarticles extraordinarily addressable, in view of standard correspondence conventions”. This infers countless heterogeneous items included simultaneously. In IoT, interesting distinguishing proof of articles and the representation and putting away of traded data is the most difficult issue. This brings the third point of view of IoT - semantic viewpoint. In Fig. 1.2, the fundamental ideas, innovations what's more, principles are highlighted and grouped with reference to the three dreams of IoT. The outline plainly delineates that IoT standard will lead to the merging of the three dreams of IoT. From the perspective of things, the centre of IoT is on the best way to coordinate bland articles into a typical structure and the things under scrutiny are radio recurrence recognizable proof (RFID) tags. The term IoT, truth be told, is credited to the Auto-ID labs, an overall system of scholarly research facilities in the field of organized RFID and developing detecting innovations. These organizations, since their foundation, have focussed their endeavours to plan the construction modelling of IoT coordinated with EPC worldwide. Thereendeavours have been principally towards improvement of the electronic item code (EPC) to bolster the utilization of RFID in the overall current exchanging systems, what's more, to make the business driven worldwide guidelines for the EPC worldwide System. These benchmarks are primarily intended to enhance object deceivability [4][5] (i.e. the traceability of an item and the attention to its status, current area and so on).

1.4.2 Applications of the IoT

The possibilities offered by the IoT make it conceivable to build up various applications in light of it, of which just a couple of utilizations are as of now sent. In future, there will be clever applications for more quick witted homes and workplaces, more brilliant transportation frameworks, more quick witted healing centres, more brilliant ventures what's more, processing plants. In the accompanying subsections, a portion of the vital illustration utilizations of IoT are quickly examined.

- Aerospace and flying industry

IoT can help to enhance wellbeing and security of items and administrations by dependably distinguishing fake items and components. The aeronautics business, for illustration, is defenceless against the issue of suspected unapproved parts (SUP). A SUP is an air ship part that is not ensured to meet the prerequisites of a sanction flying machine part (e.g., fakes, which don't fit in with the strict quality imperatives of the flying business). Along these lines, SUPs truly damage the security models of a flying machine. Flying powers report that no less than 28 mischances or episodes in the United States have been brought on by fakes [24]. Aside from tedious material investigations, checking the credibility of flying machine parts can be performed by investigating the going with reports, which can be effectively manufactured. It is conceivable to take care of this issue by presenting electronic families for specific classifications of flying machine parts, which archive their birthplace and security discriminating occasions amid their lifecycle (e.g., alterations). By putting away these families inside of a decentralized database as well as on RFID labels, which are safely connected to airplane parts, a confirmation

(Confirmation of advanced marks, correlation of the family on # RFID labels and inside of the database) of these parts can be performed before introducing them in an airplane.Thusly, wellbeing and operational unwavering quality of airplanes can be essentially made strides.

- Automotive industry

Propelled autos, trains, transports and bikes are getting to be furnished with

propelled sensors, actuators with expanded handling forces. Applications in the car business incorporate the utilization of keen things to screen and report different parameters from weight in tires to nearness of different vehicles. RFID innovation has as of now been utilized to streamline vehicle generation, move forward logistics, expand quality control and enhance client administrations. The gadgets joined to the parts contain data identified with the name of the maker furthermore, when and where the item was made, its serial number, sort, item code, and in a few applications the exact area in the office at that minute. RFID innovation gives constant information in the assembling forms, support operations and offers better approaches for overseeing reviews all the more viably. Devoted Short Range Communication (DSRC) innovation will perhaps help in accomplishing higher bit rates and decreasing impedance with other hardware. Vehicle-to vehicle (V2V) and vehicle-to-framework (V2I) interchanges will essentially progress Intelligent Transportation Systems (ITS) applications, for example, vehicle wellbeing administrations and movement administration and will be completely coordinated in the IoT framework[6][7].

1.4.3 Challenges in the Integration of Wireless Sensor Networks with Internet

. To highlight and discuss the challenges emerging from such novel responsibility assignment, we selected three potential tasks that the sensor nodes would have to accomplish: security and quality of service management, and network configuration.

- **Security**: In common WSNs without Internet access, the sensor nodes may already play an important role to ensure data confidentiality, integrity, availability and authenticationdepending on the application sensitivity. However, the current identified attack scenarios require a physical presence near the targeted WSN in order to jam, capture or introduce malicious nodes for example. By opening WSNs to Internet.

- **Quality of Service**: With gateways acting only as repeater and protocol translators, sensor nodes are also expected to contribute to quality of service management by optimizing the resource utilization of all heterogeneous devices that are part of the future Internet of Things. Not considered as a weakness, the deviceheterogeneity opens new perspectives in terms of workload distribution. In fact, resource differences may be exploited to share the current workload between nodes offering available resources. Improving the QoS, such collaborative work is consequently promising for mechanisms requiring high amount of resources like security mechanisms. Nevertheless, the existing approaches ensuring QoS in the Internet are not applicable in WSNs, as sudden changes in the link characteristics can lead to significant reconfiguration of the WSN topology. It is therefore mandatory to find novel approaches towards ensuring delay and loss guarantees.
- **Configuration**: In addition to security and QoS management, sensor nodes can also be required to control the WSN configuration, which includes covering different tasks, such as address administration to ensure scalable network constructions and ensuring self-healing capabilities by detecting and eliminating faulty nodes or managing their own configuration. However, selfconfiguration of participating nodes is not a common feature in the Internet. Instead, the user is expected to install applications and recover the system from crashes. In contrast, the unattended operation of autonomous sensor nodes requires novel means of network configuration and management [8][9].

1.5 ENCRYPTION

It is a process in which a data or a plain text is passed through a sequence of mathematical operations that develop a substitute of the original data, known as cipher text. Another way which could be used for hiding the original data using a secret key for encryption is by elaborating algorithms or applying complex programs. This encrypted data is accessible only to those parties who have been given the required key to decrypt the cipher text back into its original form. This process only makes the data hard to read, its existence is still there.

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors[10].

Encryption, without anyone else, can secure the secrecy of messages; yet different systems are still expected to ensure the respectability and validness of a message; for instance, confirmation of a message verification code (MAC) or a computerized mark. Models for cryptographic programming and equipment to perform encryption are generally accessible; however effectively utilizing encryption to guarantee security may be a testing issue. A solitary lapse in framework outline or execution can permit fruitful assaults. Here and there an enemy can get decoded data without straightforwardly fixing the encryption. It's just plain obvious, e.g., activity investigation, TEMPEST, or Trojan horse [11].

Advanced mark and encryption must be connected to the cipher text when it is made (commonly on the same gadget used to make the message) to abstain from altering; generally any hub between the sender and the encryption operators could conceivably mess around with it. Encoding at the season of creation is just secure if the encryption gadget itself has not been messed with.

Encryption has long been utilized by military and governments to encourage mystery correspondence. It is presently generally utilized as a part of securing data inside numerous sorts of regular citizen frameworks. For instance, the Computer Security Institute reported that in 2007, 71% of organizations overviewed used encryption for some of their information in travel, and 53% used encryption for some of their information in storage. Encryption can be utilized to ensure information "very still, for example, documents on PCs and capacity gadgets (e.g. USB blaze drives). Lately there have been various reports of secret information, for example, clients' close to home records being uncovered through misfortune or burglary of tablets or reinforcement drives. Scrambling such documents very still aides ensure them ought to physical efforts to establish safety fall flat. Advanced rights administration frameworks, which forestall unapproved utilization or proliferation of copyrighted material and ensure programming against figuring out (see likewise duplicate security), is another to some degree distinctive illustration of utilizing encryption on information at rest.

Encryption is additionally used to secure information in travel, for instance information being exchanged by means of systems (e.g. the Internet, e-trade), cellular phones, remote receivers, remote radio frameworks, Bluetooth gadgets and bank programmed teller machines. There have been various reports of information in travel being caught in late years.[12] Data ought to additionally be encoded when transmitted crosswise over systems to ensure against listening stealthily of system activity by unapproved users[13].

CONCLUSION

The study of wireless network with respect to internet and the aspect of security with respect to Internet of Things (IoT) are really new innovative area which requires studying more and it would be helpful for researchers to study as we have discussed above.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Comput. Netw.*, vo5no. 15, pp. 2787–2805, Oct. 2010.

[2] R. Roman and J. Lopez, “Integrating wireless sensor networks and the Internet: A security analysis,” *Internet Res.*, vol. 19, no. 2, pp. 246–259, 2009.

[3] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2139. New York, NY, USA: Springer-Verlag, 2001, pp. 213–229.

[4] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) _ cost (signature) + cost (encryption),” in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1294. New York, NY, USA: Springer-Verlag, 1997, pp. 165–179.

[5] F. Bao and R. H. Deng, “A signcryption scheme with signature directly verifiable by public key,” in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 1431. New York, NY, USA: Springer-Verlag, 1998, pp. 55–59.

[6] C. Gamage, J. Leiwo, and Y. Zheng, “Encrypted message authentication by firewalls,” in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 1560. New York, NY, USA: Springer-Verlag, 1999, pp. 69–81.

[7] Hardik Gohel, Forum Kalyani, "Li-Fi Technology– A survey on Current IT Trends", International Journal on Advances in Engineering Technology and Science Volume: 1, Issue: 2, December 2015

[8] Hardik Gohel, “Looking Back at the Evolution of the Internet”, CSI Communications-Knowledge Digest for IT Community, 38 (6), 2014

[9] Hardik A Gohel,” Cyber Security and Social Media”, CSI Communications – Knowledge Digest for IT Community, 39(5), 2015

[10] Hardik Gohel,” Introduction to Network & Cyber Security”, LAP Lambert Academic Publishing, 2015

[11] Hardik Gohel,”Data Science - Data, Tools & Technologies”, CSI Communications Knowledge Digest for IT Community, 39(3), 2015

[12] Hardik Gohel & H Molia, “Protection of Computer Networks from the Social Engineering Attacks”, International Journal on Advances Engineering, Technology and Science(IJAETS), Vol 1, Issue 1, pp 1-5, 2015

[13] Hardik Gohel,”Intelligent Web based Secure Browsing Implementation”, International Journal on Advances Engineering, Technology and Science(IJAETS), Vol 1, Issue 1, pp 14-16, 2015