ISSN 2319-2720
Volume 7, No.4, October - December 2018
International Journal of Computing, Communications and Networking
Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn02742018.pdf
https://doi.org/10.30534/ijccn/2018/02742018

Secure Communication Between Sensors in IoT

Arun Biradar[1], **Shamshekhar S. Patil**[2]
[1]Research Scholar, CSE, EWIT, Bengaluru
[1]Prof. & Head, CSE, EWIT, Bengaluru, Karnataka, India, ambiradar@yahoo.com
[2]Associate Prof. CSE, Dr. AIT, Bengaluru, India, shamshekhar.patil@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) are the foremost module of IoT that gather information from the surroundings and send the data to the destinations. A wide Varity of devices can be included in the IOT. Connecting many stand-alone IoT systems through the Internet introduces many challenges, with security being front-and-center as much of the collected information will be exposed to a wide and often unknown audience. Majority of the existing mechanisms are highly recursive that is actually not feasible for a resource-constraint node to execute for a longer run. Therefore, it will lead to an excessive shortening of resource from the sensor node thereby degrading both communication and security standard. The adversaries acts very differently in wireless sensor networks (WSN) and it has never been checked how they behave when they slipped to internet communication channel. Hence, a robust security scheme is required for securing both gateway node as well as sensor node from being prone to ever increasing level of threats in IoT network and its respective applications. The main aim of this paper is to introduce a secure communication system in IoT.

Key words: **Internet-of-Things (IoT),** Wireless Sensor Network**s (WSN), words or phrases in alphabetical order, separated by commas.**

1. INTRODUCTION

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.

IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro-services and the internet. The convergence has helped tear down the silo walls between Operational Technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.

Practical applications of IoT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation. Enterprises and users alike must be prepared for the numerous issues of IoT. Listed below some of the risks that will be inherent in an Internet of Things world, as well as suggestions to help organizations prepare for the challenge.

- Ensuring continuous availability of IoT-based devices will be important to avoid potential operational failures and interruptions to enterprise services.
- Disruptive cyber-attacks, such as distributed denial-of-service attacks, could have new detrimental consequences for an enterprise.
- Another big challenge for enterprises in an IoT environment will be figuring out how to quickly patch IoT device vulnerabilities -- and how to prioritize vulnerability patching.
- The challenges for enterprises lie in identifying where security controls are needed for this emerging breed of Internet-connected devices, and then implementing effective controls.

2. BACKGROUND

The name Internet of Things wasn’t officially so until the year 1999. At the end of the year 2013, it had evolved into a system incorporating various technologies, including the ones ranging from the Internet to communicate in the wireless field and from MEMS to embedded systems. IoT can be explored to increase the application providing capacity in multiple domains such as control systems, global positioning system, wireless sensor networks and automation.

The wireless connectivity and new techniques of digital identification like RFID got an impact of IoT on our daily lives. Due to the advancements in wireless sensor networks, and little energy, limited resource device have initiated more types of equipment that are internet connectable. To provide more addresses and unite multiple networks in the IoT environment IPv6 and IEEE 802.15.4 have been significant. Here the following shows the number of security problems in IoT. As the focuses on the analysis of real time extensive data, IoT is proved as an emerging technology. The massive amount of data is transferred to the DCNs; their underlying structures should be able to sustain the IoT data real-time processing necessities. Some of Open Challenges of IoT are:

Network Scalability: The conventional data center has three-tier topology more often to accommodate the networks from larger data centers. The architecture consists of three layers which are the access, core and aggregation layers. As the growth in the complexity and size of the increases, it leads to scalability challenges. The scalability issues arise when furthermore IoT data streams continue to flow into the warehouses. As it is one of the key essentiality to analyze the IoT real time data, it can be solved by the approach of modular data centers. For the IoT analytics, the challenge of scalability is included with reconfiguration and real-time control of infrastructure for having an agile, routing, access monitor and addressing are a demand.

Network Delay: In the present time analytics, the data flow between the switches and servers causing a delay in the system. Also, it occurs while the data is in the process of being accessed from the database. The tiered architecture of the data centers is the primary reason for a delay.

Spectral Efficiency Limitation: The massive data creates another issue for efficient delivery of data in case of real-time analytics. To avoid this, they should utilize the available range of frequencies in the network. The wireless network should have the potential of taking charge of the controlling deadlines in an analysis of real-time scenario and the data flows. Spectral efficiency as a challenge will be ineffective if the network is performing the required task.

Fault Tolerance in the Network: The functioning of an IoT system is possible only when it continuously operates even when a failure occurs for few of its components. IoT data needs a system to detect the faults and should possess the capacity of resisting it along with reporting a solution for the same.

Network Agility—applying the concept of agility in network analytics, IoT can be met with the demand for scattered sensors shared over a large pool, giving real-time services. At the availability of spare capacities in the network, congestion and computation hotspots have higher priorities. The communication among the different paths of the networks is constrained.

Some of the significant problems in IoT are as follows:

- As currently defined, IEEE 802.15.4 is unable to protect acknowledgment messages in respect to integrity or confidentiality. An adversary may therefore forge acknowledgments, for which it only needs to learn the sequence number of the packet to be confirmed that is sent in the clear, in order to perform DoS attacks.
- The challenges in the adoption of network-layer security approaches such as IPSec and IKE in 6LoWPAN environments are related to the resource constraints of typical wireless sensing platforms.
- The current RPL specification only addresses the handling of keys with applications employing device pre-configuration, discussing how such devices should be able to join a network using a preconfigured default shared group key or a key learned from a received DIS configuration message, while not defining how authentication and secure joining mechanisms may be designed to support other more dynamic or security-critical application contexts.
- Devices in future IoT applications may require mechanisms supporting the online verification of the validity of X.509 certificates, particularly for the CoAP Certificates security mode.

Hence, above mentioned points are some significant issues from a large number of security problems in IoT. The problem statement of the proposed study can be stated as follows. "*It is a computationally challenging task to design a cost-effective computational modeling of security framework considering all the operational modules in IoT to offer higher scope of security benefits*."

3. LITERATURE SURVEY

The study of Shi et al. emphasizes on encryption as a cryptographic method for the simultaneous performance of signcryption and signatures digitally. It is an effective way as it does not permit the smart device to forget or leak the confidentiality of the communication channel in the system of IoT mostly when the produced cipher texts are converted into a compact form. Implementation of signcryption is very often threatened by the device attacks captured due to the unattended signals from them ensuring that the intruder acquires the cryptographic key from the instrument which is captured.

In the study of Sajid et al., the aim is to reduce the operational expense of the industrial systems. Solutions were providing higher end stability, tolerance in the fault and flexible are required to be designed for the support. The *Cyber Physical System (CPS)* is one such technique that is the solution for the industrial systems majorly involving IoT along with the services of cloud computing. They are considered as the smart industrial system, with them being readily applicable in the field of eHealth care systems, smart grids, medical, transportation, etc. They mostly run on Supervisory Control and Data Acquisition (SCADA) systems to take charge over and monitor the Critical Infrastructure (CI). Traditional SCADA devices lack appropriate measure in security issues and hence with uniting the new architectures which are complex, the conceptualization of Mobile Sensor Wireless Sensor Networks (MWSN), cloud computing and IoT would face more challenges in security and classical system deployment in them.

Arshad et al. presents a methodology of Green IoT idea that intends on reducing the energy consumption of devices using IoT and keeping the environment safe. The different taxonomies that work in favor of the implying the Green Iot in the devices are software based green IoT, hardware-based green IoT, recycling, policy-based, awareness based and the habitat reformation towards green IoT. The influence of IoT on the economy is dominantly applied and is assumed to give an opportunity a revolution in the in the whole of ICT industry. The industry is the cause for 2% of entire CO_2emission as reported by the IEEE Green ICT report and would double in the upcoming next five years. The Green IoT is highlighted as a function of the policy established, generic architecture and recyclable material for it.

The study of Yasin et al. assures to revolutionize the sector of health care via non-invasive, continuous and remote monitoring of the patients. The two major challenges faced by the medical devices working on the principle of IoT are matter of security and privacy with energy throughput. Solutions such as low power processors of ECG and secure network protocols are the issues elaborated on these bases. Here the proposed system involves ventricular arrhythmia detection through ECG signals in a safe sensing IoT platform having ultra low-power.86% Accuracy rate is achieved when the presented method can analyze the onset of the threshold events in the cardiovascular field up to 3h. The technique is implemented utilizing an application specific integrated circuit as a function of low-power enhanced technology; the power consumption is noted to be 62.2% lesser than that consumed in the addressed approach of state of the art, having 16% smaller area size. ECG signals are used for fulfilling the requirement of the input to extract the chip-specific ECG key that allows the protection of the communication path. By collaborating the ECG core with the solution of the existing trust design, protection at the level of the hardware is attained. Efficient resource sharing is acquired in the on-chip system providing 9.5% that for the area and 0.7% for the energy with no effect on the computational speed of the IoT device.

The study of Cheng et al. discusses the mobility features and technologies in the communication domain with the constraint of the malware propagation, exploiting new challenges in the cyber security of IoT empowered malware. The difficulty arises in the process of patching the end devices under IoT when compared to those in the where nodes have the capability of directly getting repaired. As an alternative, blocking the malware through patch process enables the turning out of the result being more feasible and practical. In particular patch, nodes can in the intermediate of the function prevent the malware propagation proliferation by enabling security links infrastructure and minimizing the malware propagation in the dissemination of the device-to-device communication. A scheme to choose the useful intermediate nodes to patch, which implies to the IoT system with limited patching resources and time of response is limited. As a result, it was demonstrated that the advantage of alleviated malware propagation is obtained with the scheme of presented traffic-aware patching.

Many approaches were enabled to describe the architecture of IoT for smart applications, but a design that is holistic and comprehensive is required as shown in Table 1. The DIAT is compared with existing efforts which are proved to explore the potentiality of the challenges technically and key features of IoT .

Therefore after reviewing the existing literatures and its trends, we come to conclusion for following research gap:

- ***Vulnerable usage of Cryptography*****:** According to the existing research approaches, the cloud environment is more secured using cryptography of complex architecture; however, such forms of encryption is never possible in resource constraint nodes. Hence, good security comes at the cost of communication degradation in the form of latency as well as reduced longevity of network lifetime. In short, existing cryptographic implementation over cloud is not feasible in securing communication from sensor nodes.
- ***Error prone Public Key Encryption*****:** Existing system also leverages the utilization of public key encryption as it is widely supported by wireless sensor nodes. However, some of the public scheme e.g. elliptical curve cryptography are not reported much about their limitation. Such schemes although offer reduced key sizes but they cannot offer protection from message forgery attacks which is very frequent in denial of service attack over cloud. In short, it means the most advocated public key encryption will require amendments.
- ***Less Emphasis on Sensor's Processing Capability*****:** Irrespective of deploying homogeneous or heterogeneous forms of the sensor nodes, the networking and processing capability of each node degrades with progress of time owing to resource depletion. There is no much research work being carried out to emphasize on this aspects. The processing capability of sensor really matters when it comes to secure routing scheme. Low processing sensors are incapable of processing emergency message update and thereby have possibility to invite intrusion. Such intrusion could be avoided by identifying and replacing the low to high processing sensors. However, there is no such work in this direction.

4. PROPOSED WORK

The proposed system develops a lightweight and highly responsive encryption technique to offer minimal resource consumption from the resource-constraint sensor nodes. The significant contribution is also to introduce a novel bootstrapping key mechanism with unique generation of secret key to maintain both forward and backward secrecy. The study outcome shows that proposed system is highly practical to offer reduced resource consumption and faster algorithm processing time in presence of dynamic scenario of IoT. This work is meant for achieving the first research objective that states “To introduce a novel framework that offers secure data transmission between the sensors and internet host in IoT.”

5. METHODOLOGY

The proposed system introduces a novel mechanism of bootstrapping public keys followed by the process of sensor node enrollment within the gateway nodes. The proposed system uses Elliptical Curve Cryptography (ECC) for generating keys followed by secret key establishment as performing encryption using simplified hashing techniques. Once secure key has been established with gateway node and all its member sensor nodes than a secure grouping is applied to allocate legitimate nodes to the IoT gateway nodes. The construction of the proposed system also considers mobility of the sensor node to assess the dynamic scenarios with potential supportability of faster secret key update. The next section briefs about the significant algorithm constructed for this purpose. The proposed system uses mainly two algorithm i.e. i) algorithm for bootstrapping the key and ii) algorithm to generate secret key.

a) Algorithm for key Bootstrapping

This algorithm is executed within the gateway node which is responsible for generating a new form of preliminary secret. The algorithm considers input as α (IoT Attribute) and e (ECC tuple parameters) that after processing yields β (Bootstrapped key).The algorithm assumes an IoT attribute α as a variable that contains a set of different number of protocols executed by a gateway node (Line-1). As the proposed system uses ECC, hence, it computes the set of prime numbers that start from 2^{α} till 0. The algorithm also considers ECC tuple parameters e which is a set of many unit finite field parameters over ECC curve. Using private key K_{pr}, the proposed system uses following mathematical expression to calculate public key K_{pu},

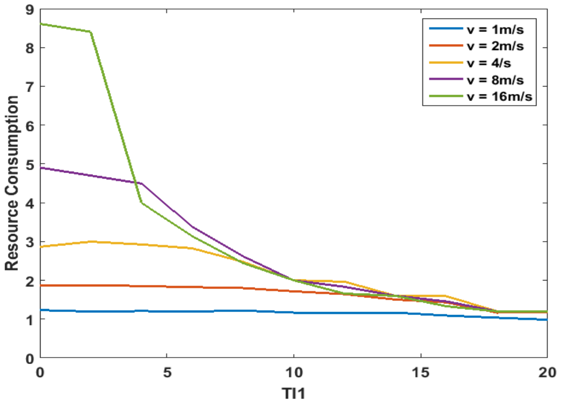
ii) Algorithm for secret key generation

This algorithm is responsible for generating a final secret key that takes input arguments of T_{range} (Transmission Range), k_{pub} (public secret key), and g (prime number). The processing yields the output of γ_2 (Secret Key). The algorithm considers all the sensor nodes N (Line-1) followed by obtaining the location information of the nodes as well as computing distance between all the other respective sensors d. All the nodes that are out of transmission range T_{range} of gateway are termed as partitioned node n_{par} (Line-2). The prime idea is to protect such node and hence a security is incorporated for such nodes (Line-3). The algorithm computes a temporary variable *id* by multiplying unique identifier *ui* with e_4. The first security token generated is γ_1 (Line-4), where the variable c_1 represents scalar product of unique node identifier, a_1, e_4, and K_{pu}, while the variable c_2 represents scalar product of unique node identifier and identifier of node with low processing capability g (line-4). The next security token is generated by scalar product of c_3 and node with low processing capability (Line-5).

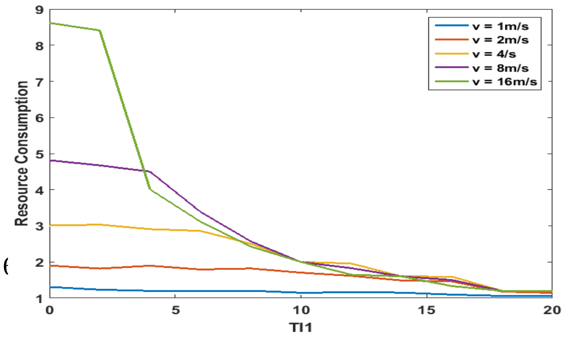
An interesting observation is that existing system has implemented 4 level of iterative steps (initialization, verification of certificate authority, mutual authentication, and hashing) in order to obtain resource consumption trend shown in Fig.1(a). On the other hand, proposed system doesn't use any form of certificates and doesn't use manifold iterative steps unlike any existing system. Hence, effectiveness of proposed system is more compared to existing system to offer similar resource dependencies but on different scale of internal operative function. Another distinct difference is that the approach of Zhao et al. doesn't offer any form of grouping mechanism for performing updating operation of secret key and such update operation is carried out by node, which also has a chance to bear any form of rogue identity. However, the proposed system offers a grouping mechanism where all the secret keys of gateway node are grouped to formed update and thereby it not only increases the security features but also offers faster operation while performing update. This feature of proposed system will assist maximum security strength compared to existing approach.

The updating mechanism of the group key is carried out when any sensor either join a new gateway during their mobility or vice-versa (i.e. depart from the old gateway node). While doing so, only the low processing sensors are priorities so that they can fulfill their task of data forwarding within a stipulated period of time. The sensor with higher processing capabilities is allowed to wait until TI1 duration. Hence, we consider another variable called as *Time Instance 2* or TI2 to represent such waiting time. Such form of scheduling while performing the key update on global scale of gateway node has not been seen in any existing authentication approach of IoT. This is quite a practical scenario that is implemented in proposed system to show that it excels less resource consumption while performing the establishment of the secret key as shown in Fig.2.

The proposed algorithm also offers approximately 49% of improvement of existing approaches on IoT. Hence, the proposed algorithm can be stated to be cost-effective security solution with faster response time.

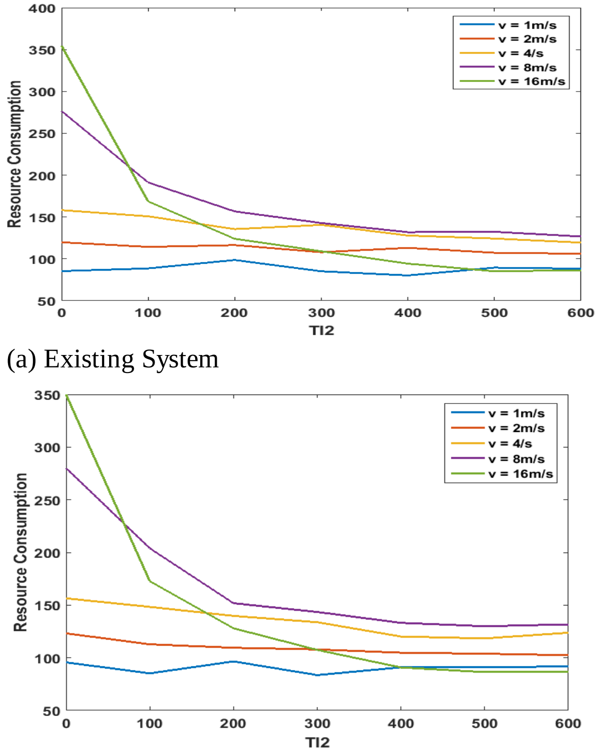


(a) Existing System



(b) Proposed System

Fig.1. Comparative Analysis of Resource Consumption for group key update



(a) Existing System

(b) Proposed System

Fig. 2. Comparative Analysis of Resource Consumption for secret key establishment

6. CONCLUSION

The proposed system has offered the solution in the form of:

- ➢ It creates a unique communication model to include both cloud and WSN environment retaining all their legacy operations connected by a gateway node
- ➢ A novel bootstrapping mechanism to generate public key to be used the gateway node for its allocated enrolled member sensor nodes
- ➢ A novel secret key generation scheme has been introduced using simple hashing mechanism.

A novel optimization algorithm will be created using message authentication code along with specifications of key expiry as well as revocation information.

ACKNOWLEDGEMENT

I would like to thank my guide Dr. Arun Biradar, Professor & Head, Department of Computer Science & Engineering, east West Institute of Technology, Bangalore, Karnataka, India for his valuable guidance and support to prepare this paper. I would like to thank all the staff members of EWIT and Dr. AIT for their support and encouragement.

REFERENCES

[1] S. ChenY. Shi, "An Obfuscatable Aggregatable Signcryption Scheme for Unattended Devices in IoT Systems", *IEEE Internet of Things Journal*, 2017

[2] Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges", *IEEE Access*, vol. 4, pp.1375-1384, 2016
https://doi.org/10.1109/ACCESS.2016.2549047

[3] R. Arshad, "Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond", *IEEE Access*, 2017
https://doi.org/10.1109/ACCESS.2017.2686092

[4] M. Yasin, "Ultra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases", *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2017
https://doi.org/10.1109/TCSI.2017.2694968

[5] S-M. Cheng, "Traffic-aware Patching for Cyber Security in Mobile IoT", *arXiv preprint arXiv: 1703.05400*, 2017

[6] S. Koteshwara and A. Das, "Comparative study of Authenticated Encryption targeting lightweight IoT applications", *IEEE Design & Test*, 2017

[7] S. Kubler, "Open IoT Ecosystem for Sporting Event Management", *IEEE Access*, vol. 5, pp.7064-7079, 2017
https://doi.org/10.1109/ACCESS.2017.2692247

[8] D. Kwon, "IoT-based prognostics and systems health management for industrial applications", *IEEE Access*, vol.4, pp.3659-3670, 2016
https://doi.org/10.1109/ACCESS.2016.2587754

[9] C. Hennebert and J.D. Santos, "Security protocols and privacy issues into 6LoWPAN stack: a synthesis", *IEEE Internet of Things Journal*, vol.1(5), pp. 384, 2014
https://doi.org/10.1109/JIOT.2014.2359538

[10] G. Zhao, X. Si, J. Wang, X. Long and T. Hu, "A novel mutual authentication scheme for Internet of Things," Proceedings of 2011 International Conference on Modelling, Identification and Control, Shanghai, 2011, pp. 563-566.
https://doi.org/10.1109/ICMIC.2011.5973767