International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Efficient Key Management for Big Data Gathering in Dynamic Sensor Networks

DHANYA S B[1], LM BERNALD[2]

[1]M.Tech computer science engineering, Rajadhani Institute of Engineering and Technology Nagaroor , Attingal, Thiruvananthapurm, Kerala, India
[2]HOD Department of computer science engineering, Rajadhani Institute of Engineering and Technology Nagaroor ,Attingal, Thiruvananthapurm, Kerala, India

---

Abstract - *Recent years have shown a huge growth in technology, which led to an explosive growth in the volume of data which is referred to as "Big Data". Wireless sensors are considered one of the highly anticipated contributor to big data nowadays, therefore, avoiding misleading or forged data gathering in case of sensitive and critical data through secure communication is vital. An efficient security schemes need to be implemented to avoid the resources consumption. Symmetric cryptography is very applicable to sensor networks due to its efficiency, which requires the use of key management for key distribution so that both communicating devices have the same key. To address that in dynamic environments, key distribution needs to be capable of accepting new devices and completing the exchange more efficiently, therefore, in this paper we propose a Centralized Stateful Connection (CSC) that provides efficient key management for dynamic sensor networks. This scheme will maintain a balance between efficiency and security that is achieved by using public key encryption .*

Keywords: **Key management, Cryptography, Wireless Sensor Networks (WSNs), CSC (Centralized Stateful Connection).**

1. INTRODUCTION

Recent years have shown high tendency towards small, inexpensive, low-power, distributed devices known as sensor nodes. Although these devices have limited processing and storage capabilities, when coordinated with each other, through their wireless communication capabilities, they can form a sensor network with the ability to measure a given physical environment in great details. One of the emerging application that attracted much attention recently is the Internet of Things (IoT) which is capable of generating massive amount of data. At the core of this technology is the sensor network, which has a high potential to improve people's lives and businesses. Although the amount of data generated by a single sensor node is not big enough to be considered as big data, the overall data generated by multiple sensors in a network can produce a significant portion of the big data. The limited resources of sensor devices (slow processor, small memory/storage, and limited power source) attracted much research attention towards this field with a focus on overcoming these limitations to improve the efficiency of WSN devices and the WSN as a whole [1] [2] [9] [10]. To support the performance of such devices, a balance between security and efficiency has to be provided. Security requirements in WSN is similar to conventional computer networks where confidentiality, availability, integrity, and authenticity must be considered when forming and building these networks. Cryptography is a popular mechanism that can provide various security services for applications and devices, but due to limitations in WSNs capabilities, not all security solutions designed for conventional computer networks can be implemented directly in WSN [5]. Symmetric encryption is considered to be faster and more efficient compared to asymmetric encryption [8]. To use symmetric encryption, two nodes are required to have the same key. This is accomplished through key management, which provides a way to distribute and manage keys between devices. Key distribution can be accomplished through a number of ways. Some of these methods are computationally expensive, which make them not very suitable for sensor networks with constrained memory, energy and processing resources. To address the aforementioned limitations, we presented a Centralized Stateful Connection (CSC) scheme that provides efficient key management for dynamic sensor networks.

2. LITERATURE SURVEY

2.1 key exchange ,authentication, and authorization in Internet of Things.

Hummen *et al.* in [3] proposed a way to accomplish key exchange, authentication, and authorization in Internet of Things. The authors discussed the use of Datagram Transport Layer Security (DTLS) and how it might be improved in terms of efficiency for constrained devices. DTLS addresses two issues that TLS cannot cope with in lossy environments; (i) independent decryption of records and (ii) unreliable delivery of messages. One of the issues with DTLS is the use of public key cryptography, which is costly and very expensive.

2.2 cluster-based key management (EECBKM) in a hierarchal WSN .

Lalitha *et al.* in [4] proposed a key management scheme called energy efficient cluster-based key management (EECBKM) in a hierarchal WSN. In their scheme, a cluster head (CH) is chosen based on the capabilities of the node. The cluster head gathers information about all the member nodes and sends the information to the base station (BS). The BS in turn will distribute cluster keys and an Exclusion Basis System (EBS) key set to each CH. Later, the CH distributes keys from the EBS keys set to each node. When a

node wants to communicate within the cluster, the node uses its key to talk to the CH. The CH grants a key to the nodes who wish to communicate. In this scheme, the nodes communicate using a key from the CH. For a node to communicate between clusters, the two CHs communicate with each other and each CH will grant a key to its node, later the two nodes will send encrypted messages through their respective CH using the provided key and the CH will deliver the message to the other CH where it will be passed to the destination node.

2.3 certificateless-effective key management (CL-EKM) scheme

Seo *et al.* in [7] proposed a certificateless-effective key management (CL-EKM) scheme. In this scheme, public key cryptography was used. In particular, this scheme uses Elliptic Curve Cryptography (ECC) with 160 bit key length. CL-EKM uses four types of keys: a certificateless public/private key, an individual node key, a pairwise key, and a cluster key. The certificateless public/private key is generated by the base station and installed in the node. This key is used to authenticate and generate a pairwise key between two nodes. An individual node key is used to encrypt communication between the node and base station. A pairwise key between two nodes is first generated using each node's certificateless public/private key pairs. After the pairwise key is established, it is used to encrypt the rest of the conversation between the two nodes. The cluster key is used to encrypt broadcast messages within a cluster. The cluster key is distributed to nodes using the pairwise key [7]. Although, the non use of certificates in CL-EKM eliminates computational overhead related to certificate management, but the overhead of the use of public key encryption remains an issue. It is worth to mention that, with the use of certificatless scheme some incompatible issues could occur where nodes might be unable to communicate with systems keys is addressed because pre-configuration can be minimized and configuration is not required within a WSN. Despite all the benefits that come with public key encryption, there still high expense when applying to WSN. Therefore, our focus is on two goals; to support a dynamic environment and to lessen the expense of security in WSN through minimizing the use of public key cryptography which will only be used once to establish the connection with the gateway. outside the network that do use certificates.

2.4 Heterogeneous network-based schemes

C. Wang, T. Hong, et al [11] used the concept of genetic algorithms to design appropriate key-generating functions for rekeying. The network consists of the sink node, headers and sensor nodes. The sink node is responsible for generating appropriate key-generating functions (sets of code slices) and distributing them to headers and sensor nodes. Each possible key generating function is encoded as a chromosome. Those chromosomes which satisfy certain power-consumption constraints and have relatively high fitness values [37] are selected for rekeying. The energy consumption of this scheme is controllable, as it only chooses chromosomes with a relative low power-consumption. However, the code-slice pool should be very large, otherwise, most of the chromosomes for different rekeying processes may be the same.

2.5 forward authentication key management scheme for heterogeneous sensor networks.

J. Y. Huang et al [12] provided a forward authentication key management scheme for heterogeneous sensor networks. This heterogeneous network includes the BS, powerful high-end sensors (H-sensors) and low-end sensors (L-sensors). The H-sensors work as cluster heads. It assumes that H-sensors can directly communicate with the BS, while L-sensors can only communicate with each other through a H-sensor. The proposed scheme loads the same hash function into the BS, H-sensors and L sensors. The BS generates key-chains for H-sensors. Thereafter, the keys in the key-chain are used for transmitting messages between a H-sensor and its member L-sensors.

3. PROBLEM DEFINITION

First in this section, we will describe our system model and notations. Then, formally we will define the research problem we are going to study. In this work the terms sensor and node are interchangeable.

Definition 1. Gateway (G): a machine on the WSN that has direct access to the internet and satisfies the conditions for a base station.

Definition 2. Base Station (BS): a machine on the WSN with a reliable power source, a sufficient security, and has more resources than nodes.

Definition 3. Node (n): a small device on the network that provides a service, typically a sensor. These devices are typically have limited resources without reliable power source.

We state the Centralized Stateful Connection (CSC) problem as the following:

Definition 4. CSC problem: Given a hierarchal wireless sensor network, where nodes are forming the lower level (leaves) of the network while the gateway/base stations form the upper level of the wireless sensor networks. The Centralized Stateful Connection (CSC) scheme seeks a centralized/dynamic key management scheme while minimizing the network's resource consumption to create a secure dynamic sensor network environment.

4. METHADOLOGY

4.1 Centralized Stateful Connection (CSC).

That provides efficient key management for dynamic sensor networks. Our scheme will maintain a balance between efficiency and security management for dynamic sensor networks. Our scheme will maintain a balance between

efficiency and security that is achieved by using public key encryption at the beginning of the node's life in the WSN and later shifts to symmetric encryption for the remainder of the communication.

4.2 key management

key management scheme. In this scheme, however, the preloaded administrative keys cannot be changed during the lifetime. As WSNs are developed, the more WSNs are developed, the more it becomes complex and dynamic. Therefore there is a need to use dynamic key management scheme that can change the administrative keys by period and on demand or upon detection of node capture. This scheme enhances the network survivability. The major concern of dynamic keying is a designing the rekeying mechanism.

5. CONCLUSION

In this work, we presented the CSC scheme which provides a way to securely exchange and manage keys in wireless sensor networks. This solution easily accommodates for a dynamic environment where nodes will enter and leave the network. We showed the performance of our proposed scheme in terms of energy consumption and provided a discussion how our scheme can help the network in overcoming different attacks. In the future, we are planning to provide more comparisons considering the security and the resource consumption aspects to show the performance of the networks with our proposed scheme.

6. REFERENCE

[1]Sangeeta Bhattacharya. Achieving Application Quality of Service in Resource- constrained Wireless Sensor Networks. PhD thesis, St. Louis, MO, USA, 2008. AAI3332063.

[2]Wan-Hee Cho, Jiho Kim, and Ohyoung Song. An efficient resource management protocol for handling small resource in wireless sensor networks. International Journal of Distributed Sensor Networks, page 9, 2013.

[3] R. Hummen, H. Shafagh, S. Raza, T. Voig,and K. Wehrle. Delegation based authentication and authorization for the ip-based internet of things. In Sensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE International Conference on, pages 284–292, June 2014.

[4] T. Lalitha, R. Saravana Kumar, and R. Hamsaveni. Efficient key management and authentication scheme for wireless sensor networks. Am. J. Applied Sci., 11(6):969–977, 2014.

[5] OWASP. Guide to cryptography. https://www.owasp.org/index.php/Guide\ to\ Cryptography, February 2012.

[6] Zhongyuan Qin, Xinshuai Zhang, Kerong Feng, Qunfang Zhang, and Jie Huang. An efficient identity-based key management scheme for wireless sensor networks by using the bloom filter. Sensors, 14(10):17937, 2014.

[7] S. H. Seo, J. Won, S. Sultana, and E. Bertino. Effective key management in dynamic wireless sensor networks. IEEE Transactions on Information Forensics and Security, 10(2):371–383, Feb 2015.

[8] J.Stretch.Symmetric encryption, asymmetric http://packetlife.net/blog/2010/nov/23/ symmetric-asymmetric-encryption-hashing/, 2010.

[9] D. Takaishi, H. Nishiyama, N. Kato, and R. Miura. Toward energy efficient big data gathering in to densely distributed sensor networks. IEEE Transactions on Emerging Topics in Computing, 2(3):388–397, Sept 2014.

[10] A. Selcuk Uluagac, Christopher P. Lee, Raheem A. Beyah, and John A. Copeland. Wireless Algorithms, Systems, and Applications: Third In- ternational Conference, WASA 2008, Dallas, TX, USA, October 26-28, 2008. Proceedings, chapter Designing Secure Protocols for Wireless Sensor Networks, pages 503–514. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[11] C. Wang, T. Hong, G. Horng, W. Wang, A GA- Based Key-Management Scheme in Hierarchical Wireless Sensor Networks, International Journal of Innovative Computing, Information and Control (IJICIC) 5 (2009) 4693{4702}.

[12] J. Y. Huang, I. E. Liao, H. W. Tang, A Forward Authentication Key Management technique for Heterogeneous Sensor Networks, EURASIP J. Wirel. Commun. Netw. 1