Review of Key Management Schemes in WSNs

Ramandeep Singh[1], Amandeep Kaur Virk[2]

[1]M.Tech Research Scholar, Department of Computer Science Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

[2]Assistant Professor, Department of Computer Science Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

Abstract: ***In this research paper we have done exhaustive study on latest key management schemes that are used in securing the WSN, however our focused in our study have been on the aspect of energy consumption due to implementation of such schemes. We have developed a comparative chart and review of all such schemes and have found certain limitations worthwhile for mentioning in this research. Based on these limitations we have also recommend certain valid points to improve key management schemes.***

Keywords: Wireless Sensor Networks, Key Management Schemes, Energy Consumption Patterns.

1. Introduction

Wireless sensor networks (WSNs) have been implemented in battlefield, hospital, forest and other crucial fields. Various attacks with the principles in computer networks pose threats to WSNs [1].WSNs consist of battery-operated sensor devices with computing, data processing, and communicating components. The ways the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical. In the uncontrolled environments, security for sensor networks becomes extremely critical [2]. Key management is the most important aspect of security in Wireless Sensor networks. Keys are also used to identify parties, which have permission to access certain information [3].

Schemes	*Features*	*Disadvantages*
SHELL [3]	1. SHELL employs EBS (Exclusion basis system) system of matrice to use small number of keys for large networks.SHELL also gets rid of single point of failure by using neighboring cluster heads for key management. 2. It is highly scalable and resilient against node capture attacks.	Its structure and operation are highly complex, involving hetrogenious node operations and multiple (at least seven) types of keys.
Eschenauer [4].	1. They have proposed a probabilistic pre-deployment scheme. Each node is loaded with a random subset of keys from a large pool. Two nodes agree on a pair wise key if both find a shared secret key in their subset. 2. This provides effective Trade-off between robustness and scalability.	It requires high memory storage requirement in a large scale wireless sensor network.
Du [5].	1.They have proposed a key management scheme based on the pair wise keying model. 2. It offers an even stronger robustness against node compromise at a reasonable scalability cost.	The main disadvantage of this scheme is its complexity, which makes it hard to implement and increase overhead costs.
Polynomial Pool Based Key Pre-distribution Scheme [6].	1. D. Liu et al. have proposed Polynomial Pool Based Key Pre-distribution Scheme that determines that Any two sensors can definitely establish a pair wise key when there are no compromised sensors. Even with some nodes compromised, the others in the network can still establish pair wise keys. 2. It allows the network to grow to a larger size after deployment.	It includes t-collision resistance (compromising more than t polynomials leads to network compromise).

Table 1: Comparison of various Key management schemes

2. Major Issues in Key Management Schemes

2.1 Security: Unreliable communication is a threat to key management in sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

2.2 Energy: Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network.

2.3 Limited memory and Storage space: A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm [7].

2.4 Integrity: With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit [7].

2.5 Data Freshness: Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack [8].

2.6 Data Confidentiality: Once the message parts are authenticated, confidentiality remains an important point. It is to keep the secrecy of exchanged messages. The confidentiality can be ensured by the use of cryptography keys (i.e. symmetric or asymmetric) [8].

2.7 Availability: Availability ensures the survivability of network services despite adversity like denial of service (DoS) attacks which may have been launched at any layer of sensor networks stack.

2.8 Self-organization: In a WSN, each node should be self-organizing. This requirement of WSN also poses a great challenge to security. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the sensors nodes [8].

3. Related work on Key management schemes

3.1 Madhuri Prashar et al. [9] have proposed in this paper about the overview and implementation of Pre-shared key scheme(PSK) in WSN and based on the results of its implementation, limitations of PSK scheme are shown in terms of connectivity and energy efficiency. To overcome limitations of pre-shared key scheme, they compare it with Binomial Pyramidal Algorithm for key management, which improves the key connectivity of WSN and make it more energy efficient. In Binomial Algorithm, the privacy of keys are between server and client. In this scheme the key distribution is at run time. The memory required for the entire simulation is less as compare to PSK. The rate of drop packets is comparatively low to PSK. There is low consumption of energy using Binomial Algorithm.

3.2 Harjot Bawa et al. [10] have demonstrate, a mathematical model of new key management scheme which overcomes the limitation of Pre-Shared key scheme, which is extensively used in wireless sensor networks. The environment of WSN is challenged by many limitations due to which there is an urgent need to manage memory which is consumed while provisioning of the key in the wireless sensor network by using N choose K algorithm. They build a more reliable network in terms of network connectivity.

3.3 Wenliang Du et al. [11] have proposed a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. They show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can he substantially improved with the use of their proposed scheme.

3.4 Gaurav Jolly et al. [12] have concentrated on the key management aspect of the security functionality using a Low-Energy Key management Protocol. Key management is essential for any cryptographic security system. They present an energy-aware approach for managing the cryptographic keys in a clustered sensor network. Shared symmetric keys are pre-deployed into the sensors and gateways (the cluster heads), requiring each sensor node to store only two secret keys. Separate protocols handle network bootstrapping, sensor addition/revocation, and key renewals.

4. Energy consumption patterns of different key management schemes

As per our systematic literature review we have come to the understanding that whenever, a key management scheme is introduced to secure the sensor network it will carry overhead in terms of energy consumption and memory. Different schemes will have different energy consumption patterns due to its complexity, level of access and security parameters. Hence, there is an urgent need to study and identify not only the strength of the key management scheme. Our attempt here is to propose and recommend models based on the disadvantages and limitations of such key management schemes.

5. Recommendations and Conclusion

Recommendations for efficient design of key management schemes are:

5.1 Ultra-low powered sensors: In WSNs the active and sleep-mode sensors are used for communication between nodes. In key management, the ultra-low powered passive sensors are used for sensing. These Sensor nodes remain sleeping until they need to undertake a specific task. At some defined time, a sensor node will wake up and perform a measurement. They are self-powered sensors. The life time of low powered sensors are more than the active sensors.

5.2 Discovery services: Given a WSN, in order to find out what services are provided by the nodes, a protocol is needed to define how the communication for discovery and usage has to take place. The two main categories of service we can identify in WSNs are reading sensors values or controlling an actuator. The aim of service discovery protocols is to facilitate the detection and the announcement of network services within a local network using key management schemes.

5.3 Unnecessary routing waste: Transmission is the most energy consuming activity a node undertakes, therefore by decreasing the number of unnecessary transmissions paths, the energy consumption in the nodes decreases significantly. In order to reduce unnecessary transmissions paths, energy-efficient data dissemination techniques have been developed to deliver the data using the minimum number of necessary transmissions [13].

5.4 Active/Passive: Sensors are classified as Active and Passive sensors. Passive sensors sense the data without actually manipulating the environment by active probing. They are self powered; that is, energy is needed only to amplify their analog signal. Active sensors actively probe the environment. Like a sonar or radar sensor, they require continuous energy from a power source. The overall work on WSNs works with passive sensors. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing [14].

6. Future Scope

Based on the recommendations and conclusions drawn from the study of key management study .We suggest for future research work that the basic pre-shared key management schemes that are using binomial distribution for security and key distribution and management must be analysed for its energy consumption pattern and further work must be improved and enhanced in such a way that its energy

consumption is reduced and no compromise on the security strength is made.

References

[1] Nanrun Zhou, Qiongxi Jiang, Xun Chen," Identity-based Key Management Scheme with Provable Security for Wireless Sensor Networks", Journal of Information & Computational Science 8: 14 (2011) 3075-3081.

[2] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz,"Security Issues in Wireless Sensor Networks", International journal of Communications, Issue 1, Volume 2, 2008.

[3] Syed Muhammad Khaliq-ur-Rahman Raazi, Zeeshan Pervez and Sungyoung Lee,"Key Management Schemes of Wireless Sensor Networks: A Survey",Security of self-organizing Networks:MANET,WSN,WMN,VANET, Auerbach Publications, CRC Press, Taylor & Francis Group,USA,2009.

[4] Shu Yun Lim , Meng-Hui Lim," Energy-Efficient and Scalable Group Key Management for Hierarchical Sensor Network", Journal of Ubiquitous Systems & Pervasive Networks Volume 2, No. 1 (2011) pp. 39-47.

[5] Johnson C. Lee and Victor C. M. Leung, Kirk H.Wong, Jiannong Cao, and Henry C. B. Chan(2007),"Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments", IEEE Wireless Communications • October 2007.

[6] Firdous Kausar,Sajid Hussain,Laurence T. Yang,Ashraf Masood," Scalable and efficient key management for heterogeneous sensor networks", Springer Science + Business Media, LLC 2008.

[7] Dr. Manoj Kumar Jain," Wireless Sensor Networks: Security Issues and Challenges", IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (Online), Volume 02, Issue 01, Manuscript Code: 110746, 2011.

[8] Abdoulaye Diop, Yue Qi, Qin Wang and Shariq Hussain", An Advanced Survey on Secure Energy-Efficient Hierarchical Routing Protocols in Wireless Sensor Networks", School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, 100083, China,2013.

[9] Madhuri Prashar and Rajeev Vashisht," Optimizing Pre-Shared Key Scheme For Effective Key Connectivity And Energy Efficiency In WSN", International Journal for Science and Emerging Technologies with Latest Trends 7(1): 1-10 (2013).

[10] Harjot Bawa, Parminder Singh and Rakesh Kumar," An Efficient Novel Key management scheme using N choose K algorithm for Wireless Sensor Networks", International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.6, November 2012.

[11] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney," A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", INFOCOM 2004.

[12] Gaurav Jolly, Mustafa C. Kuşçu, Pallavi Kokate, and Mohamed Younis," A Low-Energy Key Management Protocol for Wireless Sensor Networks," IEEE Symposium on Computers and Communications (ISCC'2003).

[13] El Jabi, Zouheir ,"Cognitive Diversity Routing in Wireless Sensor Networks", qspace.library.queensu.ca.[Online].Available: https://qspace.library.queensu.ca/handle/1974/5988.html. [Accessed: August 2010].

[14] "Sensor node", Wikipedia.com. [Online]. Available: http://en.wikipedia.org/wiki/Sensor_node. html. [Accessed: September 2009].