Grouping Applications for Appropriate Security Provision in WSN

Muhammad Zahir Shah, Aftab Alam, and Gohar Ali

***Abstract*—Wireless Sensor Networks (WSN) are gaining popularity due to their increasing use in different fields ranging from battlefield monitoring to healthcare services. WSNs are facing serious security challenges primarily due to insecure medium and unattended operations in hostile environments. Extensive studies in this regard have been done to secure WSN through different techniques. In this paper we argue that not all applications require same level of security for their proper operations, since applications do not face same level of hostile environment and motivation of attackers. In response we propose to group the applications according to security requirements which will enable researchers to better understand security issues and develop solutions as per requirements of the application and interests of an attacker.**

***Index Terms*—BROSK, elliptic curve cryptography, LEAP, public key cryptography, sensor node, trusted Server.**

I. Introduction

Wireless sensor networks consist of small sized nodes costing few cents to some dollars which are randomly deployed in large numbers in different environments to monitor some parameters, such as vibration, light, motion or sound. The storage capacity of sensor node is few KBs and normally sensor's battery last for few weeks in fully functional mode. Due to small size and limited operation; sensors have communication limitations in terms of energy, processing power, storage and communication bandwidth.

WSNs are useful in different field of life including healthcare, surveillance, fire detection and protection, environmental monitoring, military command and control, inventory control, product quality monitoring and weather forecasting [1]-[3].

Wireless sensor networks are usually deployed in hostile environment. They use wireless medium for communication which has much associated security problems. The attackers can listen what is being monitored or they can falsify the data by changing the original or injecting their own data in the network. So there is need for smarter and effective development of security policies for WSN.

The rest of the paper is organized as follow. In section two, we discuss the security related work already done in three different areas of key management schemes identifying the pioneered work done in each sub area. Section three gives a brief survey of different type of application where WSN is currently implemented and found useful. Section four discusses the applications specific security and divides the applications of WSN into three groups. In section five the evolution criteria for an application are presented and key management approach to fit the criteria. We conclude the paper in the final section.

Manuscript received September 20, 2012; revised December 10, 2012.

Muhammad Zahir Shah is with the Deptt: of Computer Science& IT, Govt. Degree College Lachi K.P.K Pakistan (e-mail: zahirktk@yahoo.com)

Aftab Alam is with the Deptt: of Computer Science & IT University of Malakand Chakdara KPK Pakistan (e-mail: alam@uom.edu.pk).

Gohar Ali is with SRC, NADRA, Peshawar K.P.K Pakistan (e-mail: gauharali@yahoo.com).

II. Security Approaches for WSN

A number of efforts have been made to secure WSNs. These efforts can be grouped into three main areas namely, Public Key Cryptography, Trusted Server Based Schemes and Key Pre-distribution. Each of these is briefly discussed in the following subsections.

A. Public Key Cryptography

The public key cryptography uses two keys, one is called public key which is known to all while the other is called private which is kept secret. RSA is widely used public key method in which security is based on the difficulty of finding prime factors of composite number. The public key cryptography is considered most expensive way of security in wireless sensor networks. However enough work has been done to optimize these approaches to be used in WSNs. The main work done in this area is by Gura *et al.* [4] which show that the Elliptic Curve Cryptography (ECC) is feasible in resource constrained sensor networks. Malan *et. al.* [5] implemented ECC in 8 bit 7.3828 MHz sensor nodes which are capable to generate keys in 34 seconds with very low storage requirements. The authors [5] have also compared two public key algorithms RSA and ECC and had shown energy consumption of key exchange on 8-bit processor.

B. Trusted Server Based Schemes

The trusted server based schemes use a trusted server to securely distribute key in sensor nodes. In these schemes the sensor nodes authenticate themselves to the trusted server and the trusted server then generate a session key and provide it to the sensor nodes for secure communication. These schemes provide very less information to attackers in case of a node compromise. However if server is compromised then the entire network will be insecure. These schemes are costly and therefore not suitable for WSN because each time new session key will be derived and distributed between communicating nodes which involve a lot of communication and processing workload that is not permissible in resource constraint WSN.

DOI: 10.7763/IJCTE.2013.V5.725

C. Key Predistribution

The third area for provisioning security in wireless sensor networks is key pre-distribution schemes which are considered most appropriate for WSNs. In these schemes some keying information is distributed among the nodes prior to deployment. This keying material is then used to generate pair wise keys for secure communication among nodes. The pioneer work on key pre-distribution was produced by Eschenauer *et al.* [6] who used the probabilistic approach for key management. Later on Chan *et al.* [7] extended the scheme and provided more strong method of key establishment. Liu *et al.* [8] has also provided a key pre-distribution mechanism for sensor networks. This area of key pre-distribution for sensor networks could further be grouped into probabilistic approaches, deterministic and hybrid approaches [9].

III. Applications of Wireless Sensor Networks

In this section we discuss some important environments for which WSNs are developed and deployed.

A. Industrial Monitoring and Control

Many industries are using wireless sensor network for information collection. The industry normally consists of large area, heavy machinery and huge man power which are monitored through a control room. The control room has many switches and indicator which tell about the status of different entities in the industry. The small and low energy sensors are put into the different parts of the factory which monitor temperature, vibration, lubricant flow etc. Such information can help to predict the failure of machine and to decide when to do the maintenance.

B. Home Automation

Home automation is an area in which wireless sensor network is widely applicable. One example could be an automatic system that operates by pressing a button resulting in switching off of all the lights and locking all the doors. The sensor indicate security problem if one or more doors remain open. The sensors in WSN for home may automatically mutes the entertainment devices when mobile phone ring or someone presses button of main gate bell.

C. Military and Warfare Applications

The wireless sensor network is used in military applications and warfare. WSN is widely deployed in battlefields to monitor and track the opponents. The information is send to the control room and appropriate action is taken against the opponents when some movement is observed in the area. The WSN could also be used for early detection and identification of biological and chemical toxic substances in the area of interest. It can help save the life of troops in biological and chemical warfare by timely and accurately detecting the type and level of toxic substances in the area [10].

D. Agriculture Field Monitoring

The agriculture scientists can benefits from the detailed data gathered through WSN about the agriculture field such as rain level, soil moisture, temperature and need for fertilizer. This information is suitable for agriculture research and will improve the productivity of the farms and agriculture field. For example if it is known that in a certain portion of the field has got heavy rain, it could be decided to irrigate only the remaining portion because irrigation is costly so money could be spend in the area that requires irrigation [11]-[12].

E. Health Monitoring

Patients health monitoring is good candidate for WSN because it can wirelessly inform the doctors and hospital staff about the condition of the patients. Tiny sensor may be used to constantly monitor the sugar level, blood pressure, weight, pulse rate and respiration rate of a particular patient and inform the related personnel about any emergency situation. They can also communicate the status and location of the patient to the emergency staff [13]-[14].

F. Environmental Monitoring

The wireless sensor network can be used to monitor habitat and fire in forest. For example, the wireless sensor network deployed on Great Duck Island helps scientists to monitor the nesting burrows of Leach's Storm Petrels without interfering the seabirds during the breeding time [13]. These sensors are placed in the nest before the bird's arrival.

Another important area is fire detection and localization in forests. The fire in forest spread very quickly especially when air blows at high rate. The sensor can detect and locate the fire and communicate the information accordingly [15].

IV. Application Specific Security for WSN

The need for security in WSNs is closely linked with the requirements of the application, the environment in which WSN is to be deployed and potential interests of the attacker. A number of security approaches have been used for WSN, but none of them consider the nature of application. Not all applications require same level of security because different applications are used for different purposes and attackers may have varying interests in interfering the mission of WSN. In this study we divided the applications of WSN into three group's namely, high security critical applications, moderate security critical applications and low security critical applications as shown in Table I.

TABLE I: The Three Secutiy Critical Applications of High, Moderate, and Low

High Security Critical Applications	**Moderate Security Critical Applications**	**Low Security Critical Applications**
Battlefield Monitoring	Health Monitoring	Habitat Monitoring
Short Term Surveillance	Home Monitoring	Agriculture Field Monitoring
Long Term Surveillance	Industrial Monitoring	Environmental Monitoring
Building security	Automatic Meter Reading	Fire Detection

A. High Security Critical Applications

Applications which require very strong security measure, usually due to manipulation of confidential information should be placed in high security critical group. The attackers have very strong interests on attacking such applications. The attackers can intercept the data, falsify the information gathered through the WSNs or even disrupt the WSNs. The battlefield is one of the areas which fall in this category. For such applications, computationally strong security mechanisms could be applied to gain better resistance. The elliptic curve cryptography is one of the choices for these applications.

B. Moderate Security Critical Applications

Moderate security critical applications are those security applications, in which attacker shows less interest due to low gain and benefit from it. However, security could not be ignored altogether. The applications like structural health monitoring, home automation, automated meter reading, industrial monitoring, healthcare, weather forecasting and inventory management can be placed in this group. For such applications, moderate security mechanism like LEAP and probabilistic key pre-distribution schemes may be implemented.

C. Low Security Critical Applications

The applications like habitat monitoring and agriculture field monitoring fall in this category. The attackers have very low gain or benefits from such WSN, so the chances of attack are also very low in these WSNs. However, security could not be overlooked altogether because there are still chances that someone could steal our important data which is collected for research purpose and get some gain from it. Computationally low security mechanisms such as BROSK and LEAP should be implemented because here the main concern is to increase the life time of WSN instead of developing very strong security.

V. Evolution Criteria for Secure Applications

Applications needs to be evaluated for resilience, scalability, storage, communication and power consumption as it will help to select a proper key management scheme which fulfill these requirements for securing each group of applications.

A. Resilience

Resilience is strength of key management schemes against an attack. A compromised key should not reveal information about other keys, for example single master key based approach fail to protect the network if a single node is captured. The higher resilience provide strong defense against network compromise.

B. Scalability

Scalability refers to the ability of key management schemes to support large number of nodes. It means that the key management schemes should be able to accommodate new node because usually node exhaust their batteries and they need to be replaced while in some cases the observed area is expanded that require additional nodes deployment.

C. Storage

Storage refers to the key management requirements of the memory. Due to resource constraint nature of WSNs, those key management schemes are preferred which have low storage requirements but higher resilience.

D. Communication Needed

Communication refers to the number of data transfers during key establishment process. The key management schemes should be able to establish keys with low communication because the energy consumption is high in data communication as compared to computation in WSNs.

E. Power Needed

The power is scarce resource in wireless sensor networks. In many situations battery of sensor nodes cannot be replaced. So the goal is to maximize the life time of sensor nodes. The security mechanism which uses less energy but provide the desired level of security is useful.

TABLE II: The Detailed Requirements of an Application

Applications	Resilience Requirements	Scalability Requirements	Storage Requirements	Communication Needed	Power needed
High Security Critical Applications	H	H	M	M	H
Moderate Security Critical Applications	M	M	M	H	H
Low Security Critical Applications	L	L	L	M	M

Table II shows the detailed requirements of an application. All the three groups of applications could be graded as high, moderate and low for required level of resilience, memory, scalability, communication and power needed. These requirements could be meet by different key management approaches.

Seyit A. Camtepe [9] has provided detailed analysis of different key management approaches which has been summarized in Table III using the scale high, moderate and low which help us to match the applications with key management schemes.

Table IV maps applications with proper key management scheme by studying the requirement of different wireless sensor networks applications from Table II and key management schemes and their scalability, resilience, memory, power and communication requirements from Table III. By matching Table II and Table III, the requirements of applications and suitable key management approaches are identified which is helpful in provisioning security in wireless sensor networks.

TABLE III: THE SUMMARY OF DIFFERENT KEY MANAGEMENT APPROACHES

Key management schemes	Scalability	Resilience	Memory	Power	communication
All pair wise	Low	High	High	Low	Low
Ransom Pair wise	Low	High	High	Low	Low
BROSK	Low	Low	Low	Moderate	Low
Light weight Key Management Scheme	Low	Moderate	Moderate	Moderate	Low
Basic Probabilistic	Moderate	Moderate	Moderate	Low	Moderate
Cluster Key Grouping	Moderate	Moderate	Moderate	Low	Moderate
Pairwise Key establishment	High	Moderate	Moderate	High	Low
Q-Composite approach	Low	Moderate	Moderate	Low	Moderate
Pairwise with Threshold	Moderate	High	Moderate	High	High

TABLE IV: MAPS APPLICATIONS

Application	Key Management Scheme
High Security Critical Applications	Elliptic Curve Cryptography, SPIN Protocol, Polynomial Based approaches, Secure LEAP, All Pairwise, Random Pairwise, Random Pairwise with Threshold.
Moderate Security Critical Applications	Localized Encryption and Authentication Protocol (LEAP),Probabilistic Approach, Random Pairwise, Polynomial Based approaches, Combinatorial Symmetric, Blom scheme, Light weight Key Management Scheme, Using Deployment Knowledge
Low Security Critical Applications	LEAP, All Pairwise (Single Key), BROSK

VI. CONCLUSION

Wireless sensor networks operate in different environments. Every sensor network application has its own level of risks and threats associated with it which depend upon the motivations and benefits of the attackers. A numbers of key management approaches exist which can help to secure the wireless networks. In this study, first the security of different applications of wireless sensor networks is analyzed and then a proper key management scheme is selected which best serve the requirement of sensor network applications in a particular context.

ACKNOWLEDGEMENT

The We are very thankful to Almighty Allah; whose grace and blessed mercy enabled us to complete this work with full devotion and legitimacy. We are grateful to Mr. Fakhruddin and Mr. Nasir Rashid (Department of Computer Science and IT, University of Malakand) for their invaluable support and guidance throughout this research work.

We also want to thank our friends and family for their encouragement; without whose support we could not have lived through this dream of ours.

REFERENCES

[1] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," in *Proc. of 1st IEEE International workshop. Sensor Network Protocols and Apps*, 2003.

[2] A. Perrig, "SPINS: Security Protocols for Sensor Networks," in *Proc. of 7th ACM MOBICOM*, 2001.

[3] L. Eschenauer and V. D. Gligor. "A Key Management Scheme for Distributed Sensor Networks," in *Proc. of 9th ACM Conf. Comp. and Commun. Sec.*, Nov. 2002, pp. 41–47.

[4] N. Gura," Elliptic curve cryptography and RSA on 8-bit CPU," in *Proc. of 6th int'l Wksp*, Cryptographic harware and embedded Sys.,Boston , MA, Aug 2004.

[5] D. Malan, M.Welsh, and M. D. Smith, "A Public-Key Infrastructure for key distribution in TinyOs based on Elliptic Curve Cryptography," in *Proc. of 1st IEEE Int'l. Conf. Commun, and Networks*, Santa clara, CA, Oct.2004.

[6] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of 9th ACM conference on Computer and Communications Security 2002*, Washington D.C., USA.

[7] H. Chan, A. Perrig, and D. Song, "Random Key Pre distribution Schemes for Sensor Networks," *IEEE Symposium on Research in Security and Privacy*, 2003.

[8] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in *Proc. of 10th ACM Conference on Computer and Communications Security*, Washington D.C., October, 2003.

[9] S. A. Camtepe and B. Yener, "Key distribution mechanisms for Wireless Sensor Networks: A Survey," Technical Report TR-05-07, Rensse laer Polytechnic Institute, March 23, 2005.

[10] C. R. Locke, G. J. Carbone, A. M. Filippi, E. J. Sadler, B. K. Gerwig, and D. E. Evans, "Using remote sensing and modeling to measure crop biophysical variability," in *Proceedings of the 5th International Precision Agriculture Conference*, Minneapolis, Minnesota, July 2000.

[11] W. Zhang, G. Kantor, and S. Singh, "Integrated wireless sensor/actuator networks in Agricultural applications," in *Proc. of the Second ACM International Conference on Embedded Networked Sensor Systems*, pp. 317, Baltimore, Maryland, USA, Nov. 2004.

[12] J. Burrell, T. Brooke, and R. Beckwith, "Vineyard computing: sensor networks in agricultural production," *IEEE Pervasive Computing*, vol. 3, no. 1, pp. 38–45, Jan-Mar 2004.

[13] T. Martin, E. Jovanov, and D. Raskovic, "Issues in Wearable Computing for Medical Monitoring Applications: A Case Study of a Wearable ECG Monitoring Device," presented at International Symposium on Wearable Computers ISWC 2000, Atlanta, October 2000.

[14] D. Malan, T. R. F. Fulford-Jones, M. Welsh, and S. Moulton, "CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care," in *Proceedings of the MobiSys 2004Workshop on Applications of Mobile Embedded Systems*, Boston, MA, June, 2004, pp. 12-14.

[15] R. W. Clay, N. R. Wild, D. J. Bird, B. R. Dawson, M. Johnston, R. Patrick, and A. Sewell, "A cloud monitoring system for remote sites," *Publications of the Astronomical Society of Australia*, vol. 15, no. 3, pp. 332–335, Aug. 1998.