ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

A Simulation Study on Scalable Key Management Scheme for WSN

Md.Anwar[1], V.Santosh Kumar[2], Sirisha K L[3]

Student, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad, India [1]

Associate Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad, India [2]

Asst.Professor, Dept. of CSE, Keshav Memorial Institute of Technology, Hyderabad, India [3]

ABSTRACT:WSN is sensitive to attacks as it is resource constrained. Network scalability is one of the concerns with respect to-secure key management schemes. Recently Bechkit et al. proposed a key pre-distribution scheme for WSN which is scalable and provides secure connectivity among nodes in WSN. They used unital design theory for key pre-distribution. Network connectivity, network resiliency, network scalability and storage overhead were the parameters used for the experiments. Influenced by those techniques, in this paper we build a prototype application, a custom simulator that demonstrates the proof of concept. The simulation involves the transmission mechanisms at sender, receiver besides the communication visualization as part of routing process. We made experiments with simulations. Our empirical study reveals that the proposed application is able to demonstrate the secure key pre-distribution process. In future it can be used to implement key pre-distribution scheme in the real world WSN applications.

Keywords: Wireless Sensor Network, security, key pre-distribution

I. INTRODUCTION

Recently, WSNs became popular as they are widely used in critical applications in various fields such as industries, healthcare, military and other civilian applications. Security in WSN plays an important role as they are sensitive to attacks. Secure key management is the corner stone of such applications where authentication is required for securing communications in WSN. As WSNs lack infrastructure, third party help can be taken for secure pre-distribution of keys. Many researchers focused in this area [12], [10], [9], [7], [4], [2], and [1]. Before looking at these researches for securing WSN communications, a typical WSN is presented in Figure 1. As can be seen, wireless sensor network is a collection of sensor nodes which can sense data about targets. The sensor nodes sense the unknown object data and send to sink node. The sink node can be accessed by authorized users through Internet. In fact the sink node can be queried in order to monitor the area under coverage of WSN.

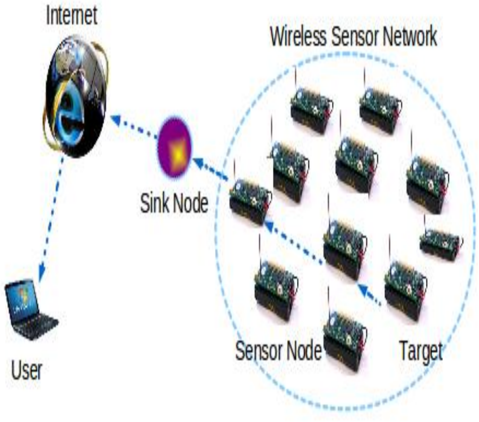


Fig. 1 – Typical wireless sensor network

In spite of many solutions on key pre-distribution, the existing solutions focused on network size and they suffer limited scalability and degraded performance. Recently Bechkit et al. [25] presented a scalable key pre-distribution scheme that makes use of unital design which maps unital design to key pre-distribution. They also explored unital – based key pre-distribution mechanism. In this paper we implement a key-distribution scheme influenced by the work in [25]. We build a custom simulator, a prototype network application that demonstrates the proof of concept. The application simulates the sender, receiver and the routing process besides key pre-distribution in scalable fashion. Our empirical results reveal that the scheme is capable of security WSN communications. The remainder of this paper is structured as follows. Section II provides review of literature on key pre-distribution mechanisms while section III bestows the proposed scheme in this paper. Section IV presents experimental results while section V concludes the paper.

II. RELATED WORK

In the literature many studies were found on key management problems in WSN [15], [14]. All the symmetric key management schemes for WSN are classified into two types namely probabilistic schemes and deterministic schemes. A direct secure key link is established between neighboring nodes in deterministic schemes while such secure connectivity is not guaranteed in probabilistic schemes. As can be seen in Figure 2, it is evident that there are many researches that belong to probabilistic schemes such as random key pre-distribution [5], [4], 3], [2], trade based key pre-distribution scheme as explored in [8], grid-based schemes for group based WSN [7], and random polynomial pre-distribution [6].

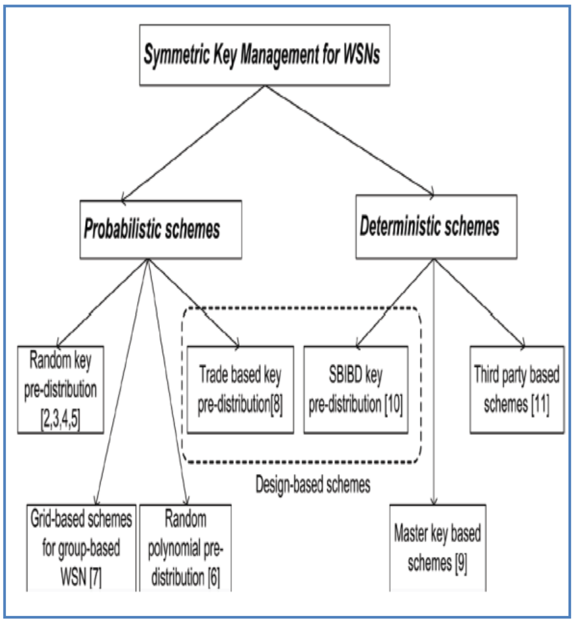

Symmetric Key Management for WSNs
Probabilistic schemes
Deterministic schemes
Random key pre-distribution [2,3,4,5]
Trade based key pre-distribution[8]
SBIBD key pre-distribution [10]
Third party based schemes [11]
Design-based schemes
Grid-based schemes for group-based WSN [7]
Random polynomial pre-distribution [6]
Master key based schemes [9]

Figure 2 – Summary of key management schemes for WSN [25]

Out of all these schemes the trade based key pre-distribution is one of the design-based schemes available. There are three deterministic schemes found in the literature. They are master key based schemes as explored in [9], SBIBD key pre-distribution as discussed in [10] and third party based schemes as presented in [11]. The random scheme assumes the knowledge of deployments. In the scheme explored in [6] bivariate polynomials are pre-loaded as keys.

III. PROPOSED KEY PRE-DISTRIBUTION SCHEME

Wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pair wise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution. The aim of the paper is to tackle the scalability issue without degrading the other network performance metrics. The mechanisms used for key pre-distribution scheme were taken from [25] where more details can be found.

As can be seen in Figure 3, it is evident that the proposed application has modules such as node deployment, key generation, key distribution, data transmission, key verification and receiving and energy computation.

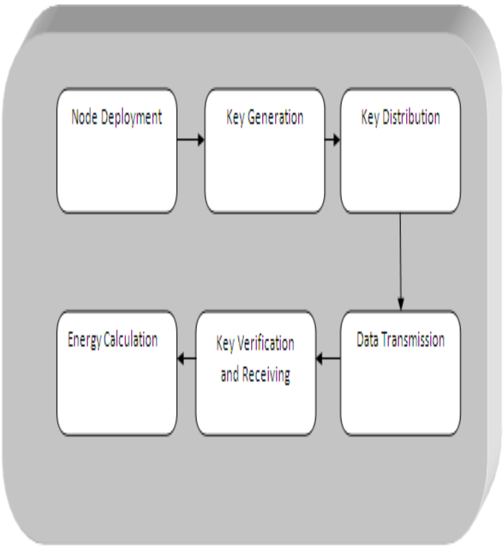


Figure 3 – Modules involved in the proposed system

These modules perform the corresponding work and the while WSN communications are secured in scalable fashion. Figure 4 shows the flow at various stages of the simulation application.

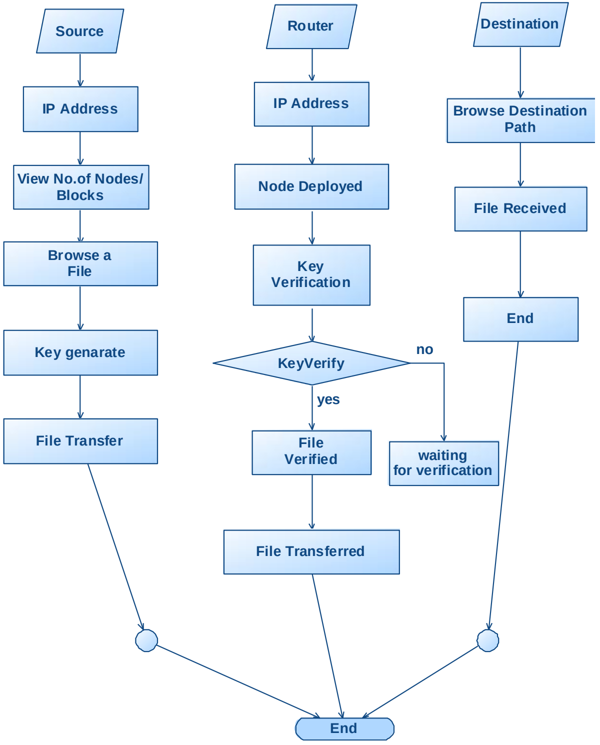
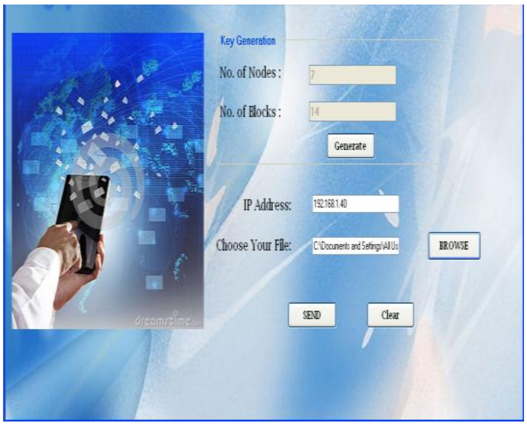


Figure 4 – Flow of the application showing source, router and destination

As can be seen in Figure 4, the proposed application has three parts that are used in simulations. The source node activities, destination node simulations and routing simulations are presented. This application demonstrates the proof of concept.

IV. EXPERIMENTAL RESULTS

Experiments are made using a prototype application, a custom simulator that demonstrates the proof of concept. The environment used to build the application is a PC with 4 GB RAM, core 2 dual processor running Windows 7 operating system. The application development environment is Visual Studio 2012 with .NET framework version 4.x. WinForms in C# is used to build user interface for simulations.



No. of Nodes : 7

No. of Blocks : 14

IP Address: 192.168.1.40

Choose Your File: C:\Documents and Settings\All Us

Figure 2 – Key generation and pre-key distribution

As can be seen in Figure 2, it is evident that the topology of WSN is created with given number of nodes and number of blocks. It also generates key and pre-distributes it. Initially the router simulation is empty and once the communication is started from a node, the router simulates the communication process in a secure fashion.

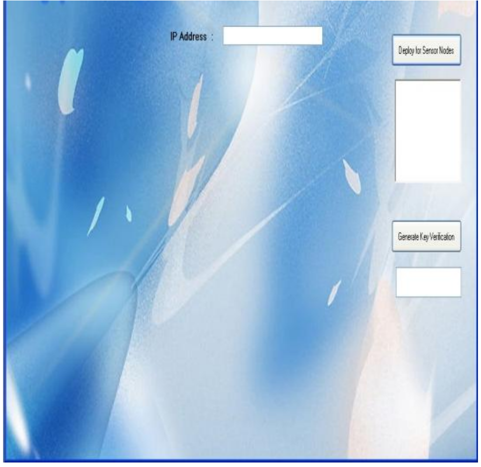
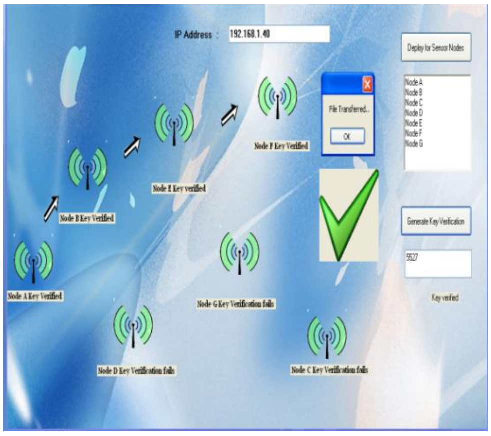


Figure 3 – Simulating router

As seen in Figure 3, the router has no simulations initially. Once a node sends communication to destination, then the simulation starts. Figure 3 shows how the data is transferred from one node to another node.



IP Address : 192.168.1.40

File Transferred..

Node A Key Verified

Node B Key Verified

Node E Key verified

Node F Key Verified

Node G Key Verification fails

Node D Key Verification fails

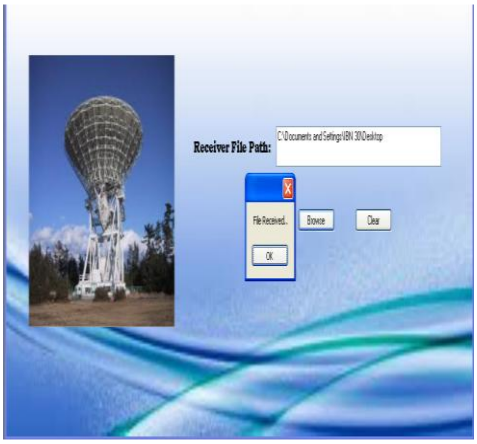
Node C Key Verification fails

5527

Key verified

Figure 4 – Router simulation with results

As can be seen in Figure 4, the router simulates communication process. From source to destination data is transferred and the same is shown graphically. The key verification is also involved in the process of simulation for security reasons. The key-distribution and verification schemes are built in such a way that they are scalable in nature.



Receiver File Path: C:\Documents and Settings\IBN 30\Desktop

File Received..

Figure 5 – Successful communication

As can be seen in Figure 5, it is evident that the simulation completes with successful communication. The same is simulated in router simulation. The communication mechanism involves key verification and the successful communication results in getting the data sent by the sender node.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we study the security problems in WSN. Especially we focus on the key pre-distribution mechanisms that are used in securing WSN communications. From the literature review it is understood that all symmetric key management schemes are classified into probabilistic and deterministic schemes. Recently Bechkit et al. [25] presented a scalable key pre-distribution scheme that makes use of unital design which maps unital design to key pre-distribution. In this paper we implement a key-distribution scheme influenced by the work in [25]. We build a custom simulator, a prototype network application that demonstrates the proof of concept. The application simulates the sender, receiver and the routing process besides key pre-distribution in scalable fashion. Our empirical results reveal that the scheme is capable of security WSN communications.

REFERENCES

[1] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” IEEE Commun. Surv. Tuts., vol. 10, no. 1–4, pp. 6–28, 2008.

[2] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. 2002 ACM CCS , pp. 41–47.

[3] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes forsensornetworks,”in IEEE SP, pp. 197–213, 2003.

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, “A key management scheme for wireless sensor networks using deployment knowledge,” in Proc. 2004 IEEE INFOCOM , pp. 586–597.

[5] C. Castelluccia and A. Spognardi, “A robust key pre-distribution protocol for multi-phase wireless sensor networks,” in Proc. 2007 IEEE Securecom , pp. 351–360.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proc. 2003 ACM CCS , pp. 2–61.

[7] Z. Yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in Proc. 2005 IEEE WCNC , pp. 1915–1920.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs," in Proc. 2011 IEEE INFOCOM , pp. 326–330.

[9] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in Proc. 2003 ACM CCS, pp. 62–72.

[10] S. A. C¸amtepe and B . Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," IEEE/ACM Trans. Netw. , vol. 15, pp. 346–358, 2007.

[11] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "Spins: security protocols for sensor netowrks," in Proc. 2001 ACM MOBICOM , pp. 189–199.

[12] B. Maala, Y. Challal, and A. Bouabdallah, "Hero: hierarchcal key management protocol for heterogeneous WSN," in Proc. 2008 IFIP WSAN , pp. 125–136.

[13] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new scalable key pre- distribution scheme for WSN," in Proc. 2012 IEEE ICCCN , pp. 1–7.

[14] J. Zhang and V. Varadharajan, "Wireless sensor network key manage- ment survey and taxonomy," J. Netw. Comput. Appl. , vol. 33, no. 2, pp. 63–75, 2010.

[15] S. A. C¸amtepe and B . Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Technical Report TR-05-07, Mar. 2005.

[16] R. Blom, "An optimal class of symmetric key generation systems," in Proc. 1985 Eurocrypt Workshop Advances Cryptology: Theory Appl. Cryptographic Techniques , pp. 335–338.

[17] T. Choi, H. B. Acharya, and M. G. Gouda, "The best keying protocol forsensornetworks,"in Proc. 2011 IEEE WOWMOM , pp. 1–6.

[18] S. Ruj and B. Roy, "Key predistrib ution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," ACM Trans. Sensor Netw. , vol. 6, no. 4, pp. 1–4:28, Jan. 2010.

[19] E. F. Assmus and J. D. Key, "Designs and their codes," Cambridge Tracts in Mathematics . Cambridge niversity Press, 1992.

[20] A. Betten, D. Betten, and V. D. Tonchev, "Unitals and codes,"" Discrete Mathematics , vol. 267, no. 1-3, pp. 23–33, 2003.

[21] J. D. Key, "Some applications of magma in designs and codes: oval designs, hermitian unitals and generalized Reed-Muller codes," J. Sym- bolic Computation , vol. 31, no. 1/2, pp. 37–53, 2001.

[22] National Institute of Standards a nd Technology, Secure Hash Standard, Federal Information Processing Standards Publication, 1995.

[23] S. Shakkottai, R. Srikant, and N. Shroff, "Unreliable sensor grids: coverage, connectivity and diameter," in Proc. 2003 IEEE INFOCOM, pp. 1073–1083.

[24] M. Doddavenkatappa, M. C. C han, and A. L. Ananda, "A dual-radio framework for MAC protocol implementation in wireless sensor networks," in Proc. 2011 IEEE ICC , pp. 1–6.

[25] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh, A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013, p948-959.

BIOGRAPHIES

Md. Anwar is currently working towards his M.Tech degree in Sreyas Institute of Engineering and Technology, Hyderabad, India. His research interests include networking and cloud computing.

Vennu Santosh Kumar received the Masters degree in Computer Science and Engineering in the year 2010. He is Microsoft Certified System Engineer & CISCO Certified Network Administrator, he worked as a System Engineer in WIPRO Technologies(INDIA). In 2011 he joined as an Associate Professor at Sreyas Institute of Engineering and Technology in Computer Science Department. He has been involved in several tutorials, workshops, technical paper presentations .His research interests are focused on Computer Networks, Network Security & Mobile Computing.

Sirisha K L S received the Masters degree in Computer Science and Engineering in the year 2010. In 2010 she joined as an Assistant Professor at Keshav Memorial Institute of Technology in Computer Science and Engineering Department. Her research interests are focused on Network Security, Information Retrieval & Machine learning.