INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

A REVIEW ON SECURE KEY RENEWAL TECHNIQUES FOR WIRELESS SENSOR NETWORK

[1]Neha Kapoor, [2]Amandeep Kaur , [3]Sushil Lekhi

[1] Rayat College of Engg. & IT, Ropar, Punjab, India,
nehak189@gmail.com
[2] Rayat College of Engg. & IT, Ropar, Punjab, India,
amandeep.banwait@gmail.com
[3] Rayat College of Engg. & IT, Ropar, Punjab, India,
lekhi.engg@gmail.com

Abstract*: Wireless Sensor Network (WSN) consists of many number of low cost, less battery-powered and self-organizing sensor nodes which are highly distributed. Forwarding attack, packet loss, malicious drop are the major threats in such a highly distributed wireless sensor network. So security applications are challenging problem nowadays in almost every network. This paper presents the information based on about WSN, its security & goals, key revocation protocol, renewing and revoking of keys.*

Keywords*: Wireless sensor network, Key renewing, Key Revocation, security, Elliptic Curve Cryptography (ECC).*

1. INTRODUCTION

Wireless sensor networks (WSNs) compose an immense number of small sensor nodes that send the collected information using the wireless channels. This sensor network is a amalgamate system combining insignificant sensors and actuate with figure out elements. Most sensor networks consist of thousands of low power, less- cost nodes expand to monitor and affect the environment. WSNs have many applications such as health monitoring, traffic control and environment monitoring of air, water and soil etc[1,2]. Most of the applications of WSNs require secure communication of information at both ends. Therefore security in WSNs is a analytical issue because sensor nodes have limited storage and energy for processing. When these sensor nodes are deployed in any environment, the problem of secured sharing of keys between sensor nodes becomes an issue of attention as sensor nodes are prone to various types of undesirable attacks [3, 4].

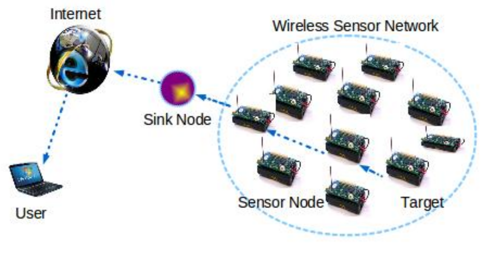

Figure 1: Wireless Sensor Network

1.1 CHARACTERISTIC OF WSN

The important characteristics of WSNs are:

- Infrastructure less
- Mobility
- Multi-Hoping
- Openness
- Network size
- Resilience Network: Capacity to cope with node failures
- Location Awareness
- Reliable transmission of Data[3]
- Fault tolerant

1.2 APPLICATIONS

WSN is very much useful in following areas.

1.2.1 Area monitoring: In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. In military, it is the used for detects enemy intrusion.

1.2.2 Environmental /Earth Monitoring: The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research including sensing volcanoes, oceans, glaciers, forests etc.

1.2.3 Industrial monitoring

- Machine health monitoring
- Industrial and control applications
- Water/Waste water monitoring
- Water distribution network management

1.2.4 Agriculture: Wireless network frees the farmer from the maintenance of wiring in an unfavorable environment. Under water systems can be monitored using pressure transmitters to detect tank levels and pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing.[6]

1.2.5 Greenhouses: The temperature and humidity levels in greenhouses are controlled by WSNs.

1.2.6 Passive localization and tracking: The application of WSN to the passive localization and tracking of non-cooperative targets has been proposed by exploiting the pervasive and low-cost nature of such technology.

1.2.7 Smart home monitoring: Smart home activities are detected using wireless sensors embedded within everyday objects forming a WSN.[7]

1.3 WSN LIMITATIONS

- Possess very little storage capacity – a few hundred kilobytes**.**
- Possess modest processing power-8MHz.
- Works in short communication range – consumes a lot of power.
- Requires minimal energy – constraints protocols.
- Have batteries with a finite life time.
- Passive devices provide little energy.[8]

1.4 WSN SECURITY

The rapidly requirements of ad hoc network technology has a wide range of applications, such as vehicular ad hoc network (VANET), wireless sensor network (WSN), emergency and military communications. Due to the features such as openness and dynamic topology, ad hoc networks suffer from various attacks in data plane.[9] WSN-based applications which induced a host of research activities in both industry and academia. Since most of the target WSN applications are very sensitive, so the major challenges in the deployment of WSN is security issue.

Goals of WSN Security

- **Message authentication**: The message receiver should be able to verify whether a received message is sent by the node that is claimed, or by a node in a particular group.
- **Message integrity:** The message receiver should be able to verify whether the message has been modified en-route by the adversaries.
- **Hop-by-hop message authentication:** Every forwarder on the routing path should be able to verify the integrity and authenticity of the messages upon reception.
- **Identity and location privacy:** The adversaries cannot determine the message sender’s ID and location by analyzing the message contents or the local traffic.
- **Node compromise resilience:** The scheme should be resilient to node compromise attacks. The remaining nodes can still be secure, no matter how many nodes are compromised.
- **Efficiency**: The scheme should be efficient in terms of both computational and communication overhead.[10]

2. LITERATURE SURVEY

Ismail Mansour et al [2014] “Secure Key Renewal and Revocation for Wireless Sensor Networks “proposed a secure mechanism for authenticated communication is deployed in a Wireless Sensor Network (WSN), several situations may arise: a node can leave the network, a new node can join the network, an intruder could try to join the network or capture a node. Therefore it is important to revoke and renew certain keys that are learned by a malicious node. We propose several secure WSN protocols for revocations and renewal of cryptographic keys in the network based on symmetric encryption and elliptic curve cryptography (ECC). For all our solutions, we provide a formal analysis of the security of our protocols using Scyther, an automatic verification tool for cryptographic protocols. All the proposed protocols are proven secure but have different security levels by using different types of keys. Finally we implemented all our protocols on real testbeds using TelosB motes and compared their efficiency.[10]”

3. PROBLEM IDENTIFICATION

In previous work several secure WSN protocols for revocations and renewal of cryptographic keys in the network based on symmetric encryption and elliptic curve cryptography (ECC) have been proposed. For all their solutions, they provided a formal analysis of the security of the protocols using Scyther, an automatic verification tool for cryptographic protocols. All the proposed protocols were proven secure but have different security levels by using different types of keys.

All results are the averages of 100 experiments of each protocol. They also provided the standard deviations for execution time including time of S. The protocol KR (key revocation) is the fastest. They also observed that almost half of the cryptographic operations are performed by sink, thus by making it doing more operations we avoid sensor nodes from doing the heavy cryptographic computations. If the size of the list of revoked nodes increases then the protocol KR will take more time. For renewing the asymmetric key they proposed four protocols, two of them use the symmetric network key NK and the other two use symmetric keys KDH. They also analyzed that since they are using the same symmetric encryption mechanism, take the same execution time. Hence, the execution time for protocols RAKnka and RAKdha is the same and similarly for protocols RAKnkb and RAKdhb. However, the second version of these protocols RAKnkb and RAKdhb are faster than protocols RAKnka and RAKdha (more so if we do not count the sink execution time). It clearly shows that the computation of the new key by a node is expensive. Therefore it is important that a designer takes it into account during the conception of the protocols in order to have efficient protocols and also to preserve resources of the nodes.

They proposed several protocols to revoke a set of nodes, and renew symmetric and asymmetric keys. All the protocols have been automatically verified using Scyther. This ensures the security of our solutions. According to the context (size of the network, size of the battery, type of mote, energy consumption for communication, computation resources of the motes) one solution might be better than another one. All these parameters should be taken into account before to choose one real solution.

3.1 ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) was developed in 1985 by Victor Miller (IBM) and Neil Koblitz (Washington University) as an alternative method for implementing public-key cryptography.

Now, we have to consider a number‘d’ within the range of ‘n’. Using the following equation(1) we can calculate the public key

$$\mathbf{Q = d * P} \qquad \mathbf{(1)}$$

d = The random number that we have chosen within the range of (1 to n-1). P is the point on the curve and ‘Q’ is the public key and‘d’ is the private key.

ENCRYPTION

Let ‘m’ has the point ‘M’ on the curve ‘E’. Randomly select ‘k’ from [1 – (n-1)].

Two cipher texts will be Calculated let it be C1 and C2, as in (2) and (3)

$$\mathbf{C1 = k*P} \qquad \mathbf{(2)}$$

$$\mathbf{C2 = M + k*Q} \qquad \mathbf{(3)}$$

C1 and C2 will be sent.

DECRYPTION

We have to get back the text ‘m’ that was send to us,

M = C2 – d * C1 (4)

M is the original message that we have send, as shown in (4).

PROOF

How do we get back the original message? Is shown in equation (5) below:

M = C2 – d * C1

'M' can be shown as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message) **(5)**

3.2 KEY GENERATION

Basically important where we have to generate both public key and private key. The source will be encrypting the message with receiver's public key and the receiver will decrypt it with its private key.

3.3 KEY REVOCATION PROTOCOL Guarantees an authenticated allocation of new keys that are efficient in terms of storage, communication and calculation overhead. The protocol minimizes the number and the size of re-keying messages. It achieves the required level of privacy and authenticity of re-keying messages by only using symmetric ciphers and one-way functions. Hence, the protocol is scalable, and particularly attractive for large and/or highly dynamic groups.

3.4 RENEWING AND REVOKING OF KEYS**:** A certificate indicates a time period during which it is valid. Attempts to utilize a certificate for authentication after or before its validity period will fail. Therefore, mechanisms for managing certificate renewal are essential for any certification management strategy. For example, an administrator may want to be notified automatically when a certificate is about to die, so that an appropriate renewal process can be finished in plenty of time without causing the certificate's subject any problem. The renewal process may involve reusing the similar public-private key pair or allocating a new one.

4. CONCLUSION

This paper gives a brief introduction about Wireless Sensor Network along with its applications and limitations. At the same time, this paper includes brief discussion on the important security aspects that are required to design a secure Wireless Sensor Network. The approaches that have been used in the literature is to optimize the size of the network, type of mote, size of the battery, energy consumption for communication, computation resources of the motes. In future we are going to analyze various key management approaches and use them to optimize the execution time for secure key renewal using Elliptic Curve Diffie Hellman algorithm in wireless sensor network with Network Simulators 2.

REFERENCES

[1] N. Akilandeswari, B. Santhi and B. Baranidharan, "A Survey On Energy Conservation Techniques In Wireless Sensor Networks", ARPN Journal of Engineering and Applied Sciences, VOL. 8, NO. 4, APRIL 2013.

[2] Mohit Saini, Rakesh Kumar Saini, "Solution of Energy-Efficiency of sensor nodes in Wireless sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[3] Wei Ye, John Heidemann, Deborah Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks" IEEE Systems Journal, No. 1, March 2013, pp26-35.

[4] Stefanos A. Nikolidakis, Dionisis Kandris, Dimitrios D. Vergados, Christos Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering", Algorithms, vol 6, 18 January 2013, 29-42.

[5] V. M. Priyadharshini, N. Muthukumar, M. Natarajan, "Cellular Architecture Sensors for Wireless Sensor Networks" IJRRSE, Vol.01 No.02, pp 47-51 June 2011.

[6] B. Baranidharan, B. Santhi, "A Evolutionary Approach to improve the life time of the Wireless sensor network" JATIT, Vol.30, pp177-183, Nov 2011.

[7] Mohd. Nazri Ismail, Abdullah Mohd. Zin, "Network Delay: how reliable network analyzer software development" IJRC, pp 9-15, 2010.

[8] B. Baranidharan, B. Shanthi, " A Survey on Energy Efficient Protocol for Wireless Sensor Network " International Journal of Computer application, Volume 11, No.10 , December 2010.

[9] Arati Manjeshwar, Dharma P. Agarwal," TEEN: A Routing Protocol for Enhanced Efficiency in WSN", IEEE 2001.

[10] Tarun Kumar Mishra , Bhupendra Singh , Arun Kumar , " A security Scheme for MANET with reduced routing overhead" , IJARCSSE , Volume 3, Issue 8 , August 2013.

[11] Ismail Mansour, G´erard Chalhoub, Pascal Lafourcade, and Franc¸ois Delobel "Secure Key Renewal and Revocation for Wireless Sensor Networks" 39th Annual IEEE Conference on Local Computer Networks.