ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on Dynamic Key Management Protocol Mechanism in WSN

Dattatray J Narale[1], Vaishali.Baviskar[2]

Student, Dept. of CS, G.H Raisoni College of Engineering and Technolohy, Wagholi, Savitribai Phule Pune University, Pune, India

Professor, Dept. of CS, G.H Raisoni College of Engineering and Technolohy, Wagholi, Savitribai Phule Pune University, Pune, India

ABSTRACT: Now a days due to advancement in wireless communication it has enabled the design and development of wireless sensor networks with less cost, less energy consumption and high utilization. A lot of cluster-based wireless sensor network routing protocols techniques have been implemented. The most of them take little consideration on communication protection, which is valuable to ensure the network security. In this paper, we implement a certificate less-effective key management mechanism (CL-EKM) protocol for secure communication in dynamic WSNs useful by node mobility. The CL-EKM supports efficient key renovate when a node leaves or joins a cluster and ensures forward and backward key secrecy in WSN. The protocol helpful for efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links as the network consideration. A security analysis of our scheme shows that our protocol is effective in defending against various attacks which is happened in network. We develop CL-EKM in Contiki OS and simulate it acceptingCooja simulator to assess its time, energy, communication, and memory performance respectively.

KEYWORDS- Wireless sensor networks, key management, clustering, certificate less public key cryptography, security and confidentiality.

I. INTRODUCTION

Dynamic WSNs are promptly updated in monitoring applications, such as target tracking in battlefield surveillance, healthcare systems technique, traffic flow mechanism and vehicle status monitoring, dairy cattle health monitoring [5]. The sensor devices are vulnerable to malevolent attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments scenarios and lapses of connectivity in wireless communication [2]. Thus, security very valuable issues in many critical dynamic WSN applications in WSN aspect. Dynamic WSNs thus need to address key security conditions, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move anywhere in the network.

Wireless sensor networks (WSN) are wireless networks design of spatially distributed autonomous devices mechanism using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration techniques, pressure techniques, motion or pollutants, at different locations and different time. Every sensor node in a sensor network is typically rigged with a radio transceiver or other wireless communication device generally, a small-scale microcontroller, and an energy source, techniques normally a battery. The implementation of WSNs were originally motivated by military applications such as battlefield surveillance scenarios, however, due to the deployment flexibility and maintenance simplicity, wireless sensor networks are now essential in many civilian application areas, including environment and habitat categorization monitoring, healthcare applications, home automation, and traffic control systems. As the applications gain more ground, security issues have also become a hot research topic. In [1], a resource oriented security solution (ROSS) was introduced to assure the network connectivity of composite clustered sensor networks (HCSNs). The security analysis and performance simulation show that ROSS not only administer the predefined security

DOI: 10.15680/IJIRCCE.2015. 0311149

and authentications objectives, but also grant a tradeoff between security and performance cost. In [2], three new enhancement mechanisms in the framework of random key redistribution were proposed to address the bootstrapping issue, namely the q-composite scheme, the multipath reinforcement technique, and the random pairwise mechanism. Each of these three techniques represents a different tradeoff in the design space of random key protocols. Eschenaueret al. implemented a key management mechanism for distributed sensor networks [5]. The technique is designed to satisfy both operational and security requirements respectively. It relies on probabilistic key distribute among the nodes of a random graph and handling simple protocols mechanism for shared-key analysis and path-key establishment purpose, and for key revocation, re-keying, and incremental addition of nodes in a WSN. Paper [6] Implemented the localized broadcast authentication in huge sensor networks to take complete advantage of roles of network nodes and limited data in a sensor network by considering WSN mechanism, and to provide an different solutions regarding accord between verification delay and broadcast overhead for satisfying applications with contrasting requirements. The updated protocol was implemented in [4] to construct the shared session key in wireless sensor network. This protocol has more scalability in simulation because the time needed to finish key negotiation does not rely on the number the sensor nodes. It can also recover power by reducing the number of transmissions.

II. RELATED WORK

1. A DYNAMIC CLUSTER-BASED KEY MANAGEMENT PROTOCOL IN WIRELESS SENSOR NETWORKS [1]

From this paper we Referred-

As the function of wireless sensor networks achieve more ground, security issues have also become an important research topic. This paper discussed the clustered WSN key management protocols and proposed a new protocol which is essential for the key management of dynamic clustered networks, based on their operation techniques. The developed protocol addresses the network security issues with cluster head update. It is differentiate with low power consumption, less computation workload and improve security. Besides, the protocol uses a symmetric key system, and consists of the sub-protocols that implement how keys are distributed, added, revoked, and updated during the life time of the sensor network. The protocol assumes that each sensor node is able to get its location information, which is currently a major restriction to its application. Our next target is to design and implement an experiment software system to quantitatively study the proposed protocol's performance and compare it with that of other existing protocols available in the market.

2. KEY MANAGEMENT ISSUES IN WIRELESS SENSOR NETWORKS CURRENT PROPOSALS AND FUTURE DEVELOPMENTS [2]

From this paper we Referred-

In this paper, we observe five key management schemes starting with the classic Eschenauerscheme and moving to the more recent schemes published in 2006. It is clear that plentiful tradeoffs exist between different key management schemes, and the vast number of proposals makes it difficult to compare them in WSN aspect. Now day's trends also show that cluster or group operation is an essential feature that has been considered by many recent key management proposals including LEAP, SHELL, and Panja's mechanism.

3. A NEW KEY ESTABLISHMENT SCHEME FOR WIRELESS SENSOR NETWORKS[3]

From this paper we Referred-

In this paper, we propose a new technique that can be used for establish various keys(pairwise keys, path keys and group keys) for wireless sensor networks. It can accomplish quick authenticity without extra computations and communications. The experiment output shows the performance of TKLU is invigorating.

4. ANALYSIS OF KEY MANAGEMENT SCHEMES IN DYNAMIC WIRELESS SENSOR NETWORKS [4]

From this paper we Referred-

In this paper we observe the mechanism of the dynamic key management techniques in wireless sensor networks, as well as their advantages and shortcomings. The vital advantage of We simulated all the four techniques in order to compare the energy consumption of each of the mechanisms.

5. DYNAMIC KEY MANAGEMENT IN WIRELESS SENSOR NETWORKS: A SURVEY [5]

From this paper we Referred-

In this paper, we developed dynamic key management schemes in WSNs. With the wide application of WSNs, as one of the crucial security issues, dynamic key management is attracting more attention from the researchers and industrial engineers and many mechanisms were already developed. We conclude the basic requirements of dynamic key management in WSNs, surveyed the developed schemes for these environments and highlighted the security and performance advantages and disadvantages of each technique. At the last, we have summarized and analyzed these techniques according to the discussed evaluation metrics in WSN aspect. In summary, it is not possible to and one single perfect scheme can implement well in all evaluation metrics as each of them has some definite strengths, weaknesses and suitability for specific scenarios. The ultimate aim of this study is to encourage more researchers to design and enhance potential proposals in dynamic key management for wireless sensor networks.

6. ENERGY EFFICIENT KEY MANAGEMENT ANALYSIS USING AVL TREES IN WIRELESS SENSOR NETWORK [6]

From this paper we Referred-

Our mechanism improves Blom’s scheme by minimizing the storage required by using a modified sparse Hadamard matrix & eliminates the run time generation of public matrix to save the computational time & computational energy of the energy scarce sensor nodes which is very essential in WSN. The wireless communication cost is diminished by the reduction of the data packets, and the clustering protocols enhance the lifetime and the energy consumption of the networks by data aggregation in wireless sensor networks. That’s why; we have only taken the dynamic WSNs in the consideration. In this paper, we developed a novel key management technique for dynamic WSNs security using balance factor in hexagonal network topology. Additionally, during the node dynamic update stage, we add the idea of the self-balanced binary search tree to assure the dynamic security of the network while minimize the entire cluster node energy consumption.

III. SCOPE OF RESEARCH

The scope of our proposed approach is to implement,two-layered key management technique and a dynamic key update protocol mechanism in WSNs based on the Diffie-Hellman (DH), respectively. However, both schemes are not matched for sensors with defined ways and are unable to perform expensive computations with large key sizes (e.g. at least 1024 bit). Since ECC is computationally more powerful and has a short key length (e.g. 160 bit), many other approaches with certificate have been developed based on ECC. However, since each node must exchange the certificate to provide the pair-wise key and authenticate each other’s certificate and data before use, the communication and computation overhead improve dramatically. Also, the BS suffers from the overhead of certificate management which is very important in WSN scenarios. Moreover, existing schemes are not secure and authenticated

IV. PROPOSED METHODOLOGY AND DISCUSSION

In this paper, we develop a certificate less effective key management (CL-EKM) mechanism for dynamic WSNs. In certificate less public key cryptography (CL-PKC), the user’s private key is a merging of a partial private key construct by a key generation center (KGC) and the user's own secret value with respect to WSN. The special organization of the full private/public key pair removes the necessity for certificates and also resolves the key escrow errors by removing the authority for the user's full private key. We also take the advantages of ECC keys which are defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length.

SYSTEM FLOW

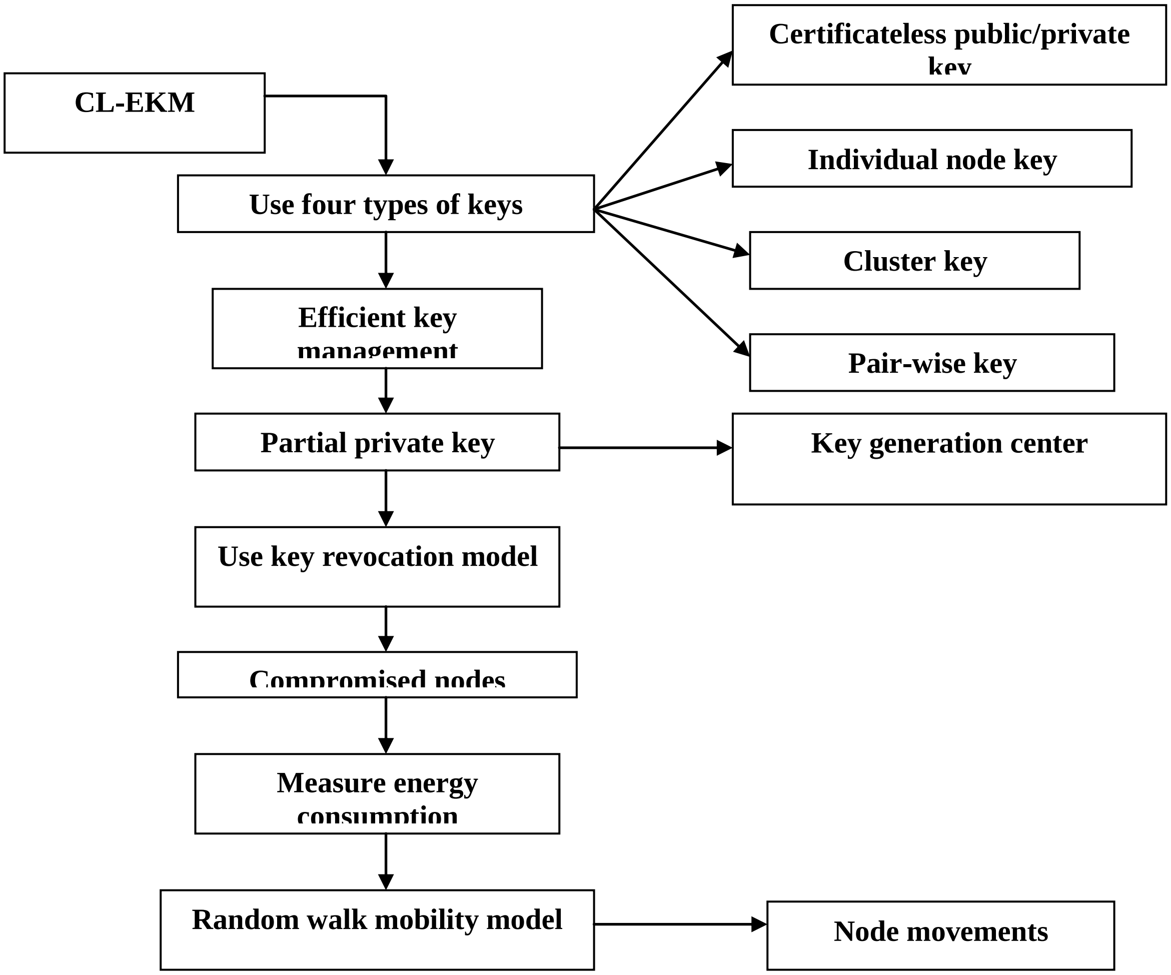

Fig No 01

V. CONCLUSION

From the consideration of all the above points we conclude that we develop the first certificate less effective key management protocol techniques (CL-EKM) for the purpose of secure communication in dynamic WSNs. CL-EKM helps

DOI: 10.15680/IJIRCCE.2015. 0311149

for efficient conversation for key updates and management in dynamic WSN when a node leaves or joins a cluster in WSN and hence ensures forward and backward key secrecy in WSN mechanism. Our approach is resilient against node compromise, cloning and impersonation intrusion and secures the data confidentiality and integrity also. The experimental results demonstrate the performance of CL-EKM in resource constrained WSNs.

REFERENCES

1. Lin Shen And Xiangquan Shi "A Dynamic Cluster-Based Key Management Protocol In Wireless Sensor Networks" International Journal Of Intelligent Control And Systems Vol. 13, No. 2, June 2008, 146-151
2. Johnson C. Lee And Victor C. M. Leung "Key Management Issues Inwireless Sensor Networks: Current Proposals And Future Developments" 1536-1284/07/$20.00 © 2007 Ieee
3. Eric Ke Wang, Lucas C.K.Hui And S.M.Yiu "A New Key Establishmentscheme For Wireless Sensor Networks" International Journal Of Network Security & Its Applications (Ijnsa), Vol 1, No 2, July 2009
4. Seyedhossein Erfani1, Hamid H. S. Javadi2 "Analysis Of Key Management Schemes In Dynamic Wireless Sensor Networks" Acsij Advances In Computer Science: An International Journal, Vol. 4, Issue 1, No.13 , January 2015issn : 2322-5157
5. Xiaobing He_, Michael Niedermeier And Hermann De Meer "Dynamic Key Management In Wireless Sensor Networks: A Survey" Preprint Submitted To Journal Of Network And Computer Applications April 26, 2013
6. Ushamrobinchandra Singh1, Kh. Manglem Singh2 "Energy Efficient Key Management Analysis Using Avl Trees In Wireless Sensor Network" International Journal Of Engineering Science Invention Issn (Online): 2319 – 6734, Issn (Print): 2319 – 6726