A Survey on Dynamic Wireless Sensor Network for Certificate-less Effective Key Management

Swapnil B. Kamble

SKNCOE Pune, Maharashtra, India.

swapnilkamble0506@gmail.com

Abstract - The Security Key management scheme has wide coverage for problems regarding WSN because the sensor nodes may be physically attacked by an intruder. The several key management techniques that present security and operational necessities are proposed in a recent network. The WSN have been used in various type of dynamic applications, for example, area monitoring, industrial monitoring, patient health monitoring, traffic surveilling, some sensor devices are mobile so they are move from one location to other. WSN comprises small sensor nodes with computation capabilities, strained energy and memory. Encryption key protocols are applied for securing data and communication. This work presents an idea of CL-EKM protocol for secure communication in WSN differentiated by node mobility. The CL-EKM supports efficient key updated when a new node join a cluster key revocation when the node is attacked by an intruder. Key revocation is occurring to minimize the effect of node compromise in active communication. Efficient key management also supports forward backward key secrecy. A security analysis of this method introduced effectively in a struggle against a various multi-hop wireless network.

Keywords — Certificate less Cryptography, Cluster, Public Key Cryptography, Sensor, Wireless Sensor Network

I. INTRODUCTION

Different applications in the range of WSN has got consideration towards the accessibility of strong public key cryptography. The most important benefit of PKC is the availability of authentication key exchange between sensor nodes that are more secure and reliable compared to secret key cryptography. Still, besides the beneficial, the PKC has an important disadvantage is, it is computationally expensive. It is conceivable to apply it, however, the question that remains is that by which the use of strong public-key cryptography influences the lifetime of the energy source and the sensor. That is why here proposed scheme tries to find the costs of public key cryptography in WSN and their affect to the node lifetime. This distinguishes between energy consumed for the calculation and energy used to transfer calculated results. Proposed scheme present a certificate less effective key management scheme for dynamic WSN. In certificate less public key cryptography, the users full private key is a combined with partial private key generated by a key generation center and the users own secret value. The organization of the full private/public key pair removes the need of certificates and also resolves the problem of key escrow by removing the authority for the users full private key. The benefit of Elliptic Curve Cryptography keys defined on an additive group with a 160-bit length as secure as the secure random keys with 1024- bit length. Energy preservation for WSN. In proposed scheme shortest path algorithm compute shorter communication link for packet sending.

II. REVIEW OF LITERATURE

In wireless sensor network, sensor nodes are mobile so nodes may move one location to another location. For secure communication requires suitable encryption/ decryption key

protocols. Proposed CL-EKM protocol for secure communication in dynamic wireless sensor network featured by node mobility. The Certificate less approach supports efficient key manipulation when a node added or removed a cluster and assures key secrecy. The protocol supports efficient key revocation for compromised nodes and reduces the effect of a sensor nodes compromise on a security of other communication networks. A security evolution of proposed scheme shows that this protocol is effective in avoiding different attacks. Proposed simulation is done using Cooja simulator to assess its memory performance, time, communication, energy [1]. Efficient key management in wireless sensor network is a big problem due to asymmetric key cryptography is not flexible in resource-limited sensor nodes and also sensor nodes are physically compromised. So to avoid this problem first, in the q-composite keys scheme, which reduce a big-scale network attack in order to strengthen the random key pre-distribution scheme against different intruder attack is applied. The random pair-wise key scheme, which excellently preserves the secret of the entire network, if any of the sensor nodes is compromised and also enables hop-to-hop authorization and key revocation [2]. To attain security in WSN, it is necessary to be use encryption over messages sent between sensor nodes. Communicating nodes must be authenticate encrypted node. Achieving key agreement in WSN is non-trivial because of resource constraints. Many key agreement techniques used in wireless networks, for example, Diffie-Hellman and public key cryptography are not useful in WSN. Pre-distribution of confidential keys for all nodes is unreliable due to a big amount of memory used while network is big. Random key distribution before packet transmission mechanism and its improvement has been invented. Proposed scheme assume that random key pre-distribution scheme is that no deployment knowledge is available. In much approaches, certain deployment knowledge may be available a priori. It presents the performance of WSN can be mechanically improved [3]. Interconnection of a remote users with sensor nodes is achieved and proposed a new lightweight authorization scheme used to the resource constrained environment. This scheme establish the secure communication after a sensor the remote user to verify each other. This technique defines non-useful, Keyed-Hash message authentication to verify the integrity of the various exchanges. This scheme proposes that it provides authentication with minimum energy consumption and it ended with a session key agreement between a sensor node a remote user [4]. Proposes a multiplication in GF(2163) using a similar multicore microcontroller. This work achieves performance results and compares these to the sequential implementation of combo multiplications with and without modular deduction for different word size 8, 16 and 32 bits on single core microcontrollers. Proposed scheme obtains results outperform most of the published single core modular multiplication implementations and require much fewer cycles [5]. Probabilistic key based mechanism for wireless communication using a slow re-keying path key reestablishment methodology. A method to redesign the existing ordinary re-keying technique of probabilistic key management techniques by a deterministic algorithm that works on both base station and on every communicating pair of sensor nodes is achieved by developing a novel, energy efficient, distributed faster techniques [6]. Proposed a protocol Mobile Open Infrastructure Network Protocol for non-synchronized UWB based wireless network communication is applied [7]. In the distributed WSN robust detection of a change in a parameter of auto regressive model. Proposed scheme is robust on the single sensor level by suppressing the effect of outliers and impulsive noise via a shortest (Energy efficient) distance metric between the long-term the short-term auto regressive model [8].Proposed scheme presents clone node attack detection where work has been done for the prevention of this attack in mobile WSN. Consequently, in this technique author present an approach to prevent Clone Node Attack in mobile WSN where the proposed scheme does not use sensor nodes private data log (location information) [9]. Paper present two key pre-distribution techniques that enable a moving sink to create a

secure data communication link, with any wireless sensor node. The proposed technique is based on a polynomial pool based key pre-distribution scheme, a q-composite scheme, a probabilistic generation key pre-distribution scheme. The security techniques shows that these two proposed pre-distribution schemes guarantee, minimum communication overhead, high probability that any sensor node can create a pair-wise key with a mobile sink [10].

III. SYSTEM ARCHITECTURE

Proposed architecture address the problem for security verification without using certificate less key management. In this proposed system different key management techniques are designed which includes individual key, pair wise key, cluster key, public key private key cryptography for effective secure key management. In node to node communication respective keys are verified for packet transmission. Dynamic key management scheme ensure the node verification at multipath routing for active source routing. This architecture also contributes for multi hop node confidentiality by adding extra noise to packet data. This noise may be extra bit added to original data or packet.

This scheme follows:

1) The protocol have to create the key between all sensor nodes which have to exchange data securely.
2) Addition of new node have to be supported.
3) It should work in undefined deployment environment.
4) Unauthorized nodes restricted to communicate with network nodes.
5) Multi-hop node confidentiality by maintaining previous node secrecy.

Security is very useful as a key challenge to the deployment of WSN. More security schemes developed for networking environment don't take into account the distinctive features of wireless sensor networks: PKC is computationally impracticable due to the limitations applied on power consumption the physical memory of the individual sensor. This WSN schemes provide the security to securing data and communications.

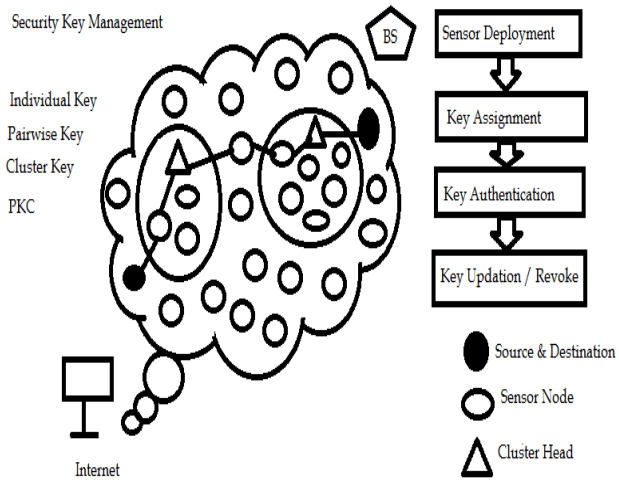

Fig. 1. System architecture of Security management.

IV. RESULT ARCHITECTURE

Effective key management scheme is designed for implementing security mechanism by key authentication scheme along with energy efficient packet transmission in WSN. In secure wireless sensor network efficiency is measured by maximization of throughput by reducing packet loss ratio and improving packet delivery ration in network.

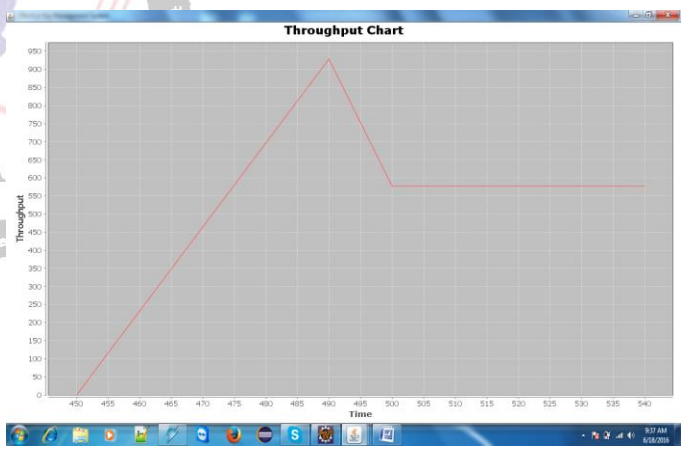

Fig. 2. Communication throughput for session authentication.

Above figure shows maximized throughput in packet transmission with effective key management techniques.

In above figure only throughput is shown we can also measure the result using delay in packet transmission, delivery ratio, loss ratio and overhead.

V. RESULT TABLE

In this section performance metrics are used to evaluate performance of routing protocols and data dissemination protocols scheme when no in networking processing is performed and no caching is used.

Goals	Existing System	Proposed System
Throughput	80	90
Network	Hop By Hop Network	Queue based Response
Controller	KGC	Key Authentication
Security	ECC Based	Secure Random Key
Protocol	PKC	Radio Resource Control

Table 1. Result Table

VI. CONCLUSION

The proposed system designs first certificate-less key management (CL-EKM) system protocol for secure key management. Certificate-less key management system manages key updation and management when new node joins the cluster or when node leaves the cluster by ensuring backward and forward key secrecy. This scheme is versatile against node copy, node compromise network attacks. Scheme protects the data confidentiality and integrity. The experimental result shows the energy efficiency of CL-EKM system in the resource constrained wireless sensor network. This system implements active trust routing for energy efficient packet transmission. Security key plays vital role in sensor nodes authentication and authorization in wireless network communication. Dynamic sensor network uses sensor deployment for improving network lifetime. Here in this network density monitored area to determine optimal sensor deployment.

REFERENCES

[1] S. H. Seo, J. Won, S. Sultana and E. Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371-383, Feb. 2015.

[2] A. Rasheed and R. Mahapatra, "Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 1, pp. 176-184, Jan. 2011.

[3] Z. Yu and Y. Guan, "A key pre-distribution scheme using deployment knowledge for wireless sensor networks," IPSN 2005. *Fourth International Symposium on Information Processing in Sensor Networks*, 2005., 2005, pp. 261-268.

[4] H. Khemissa and D. Tandjaoui, "A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of Internet of Things," 2016 *Wireless Telecommunications Symposium (WTS), London, 2016*, pp. 1-6.

[5] M. S. Albahri and M. Benaissa, "Parallel comba multiplication in GF(2163) using homogenous multicore microcontroller," 2015 *IEEE International Conference on Electronics, Circuits, and Systems (ICECS), Cairo*, 2015, pp. 641-644.

[6] S. Biswas, M. M. Haque, S. Rashwand and J. Misic, "Fast, Seamless Rekeying In Wireless Sensor Networks," 2009 *29th IEEE International Conference on Distributed Computing Systems Workshops, Montreal, QC, 2009*, pp. 166-171.

[7] M. Janssen, A. Busboom, U. Schoon, G. von Colln and C. Koch, "A mobile open infrastructure network protocol (MOIN) for localization and data communication in UWB based wireless sensor networks," 2014 *IEEE International Conference on Ultra-WideBand (ICUWB), Paris, 2014*, pp. 409-414.

[8] D. Kalus, M. Muma and A. M. Zoubir, "Distributed robust change point detection for autoregressive processes with an application to distributed voice activity detection," 2015 *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, 2015*, pp. 3906-3910.

[9] M. Qabulio, Y. A. Malkani and A. Keerio, "Securing mobile Wireless Sensor Networks (WSNs) against Clone Node Attack," 2015 *Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 2015*, pp. 50-55.

[10] O. Yagan and A. M. Makowski, "Wireless Sensor Networks Under the Random Pairwise Key Predistribution Scheme: Can Resiliency Be Achieved With Small Key Rings?," in *IEEE/ACM Transactions on Networking, vol. 24*, no. 6, pp. 3383-3396, December 2016

