IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A Certificate Less Active Key Management in Dynamic Wireless Sensor Networks

Priyanga Ancy.G[1], Narmadha.C[2]

PG Student, Dept. of ECE, Periyar Maniammai University, Thanjavur, Tamilnadu, India[1]

Assistant Professor, Dept. of ECE, Periyar Maniammai University, Thanjavur, Tamilnadu, India[2]

Abstract: Wireless sensor networks (WSNs) to replied continuous accessibility of the wireless medium to communicate contributing the sensor nodes. Though, the open nature of this wireless medium leaves it exposed to multiple security threats or attacks. The encryption key protocols are required to securing data and communications. Symmetric key schemes are unworkable for mobile sensor nodes and therefore past methods have concentrated only on static WSNs. It is also not mountable and not strong compared to compromise nodes, and not capable to support node mobility. Hence symmetric key is apposite for dynamic WSNs. Extra in recent times; asymmetric key based methods must be present future for in dynamic WSNs. In this paper, a Certificate less Active Key Management (CL-AKM) protocol to supports key revocation in dynamic WSNs is proposed. The proposed scheme is secure communication in dynamic WSNs and categorised by node mobility. Key updated after a node movement of node leaves or node connections a cluster and key revocation for compromised nodes are supported by our proposed scheme and ensures go forward and backward key confidentiality. Our proposed scheme of security research is effective in a number of attacks. We implement and simulate the Certificate less Active Key Management (CL-AKM) protocol using NS2 simulator to assess its energy, delay and threshold.

Keywords: CL-AKM; Security; Key Management; AODV protocol; Node Mobility.

I. INTRODUCTION

A wireless sensor network (WSN) is a network designed by a huge amount of sensor nodes, each armed with sensor(s) to identify physical phenomena such as temperature, light, motion, or sound. The WSN is manufactured by a "nodes" from a rare to some hundreds or equal thousands, wherever each node is attached to one sensor. A WSN node is also known as mote, it is commonly providing with one or numerous sensors to get data about the neighbouring environment. The different sensors to use, WSNs can be executed to support many applications composed with security, entertainment, military sensing and tracking, patient status monitoring, automation, industrial monitoring, traffic flow monitoring, public utilities, and asset management. Though, many WSN devices have simple source constraints in terms of energy, threshold, computation, and memory, produced by a requirement to limit the cost of the large number of devices essential for various applications and by arrangement settings that avoid easy admittance to the devices. Such resource limitations are too many open problems as well as WSN security which have been considered dynamically by investigators. Various applications want WSNs is to exchange complex data or contain opinion methods that require high reliability requests, and they require a high level of security to be successful. However, strong security is difficult to complete with source-incomplete sensor nodes, and various well-known methods become infeasible. Wireless Sensor Network has much particularity that finished them very vulnerable to malicious Attacks in unapproachable Surroundings like military battleground [1]. Data confidentiality is a fundamental security service to presence the secrecy of dynamic data transmitted between sensor nodes [3], [11]. A key-chain distribution system for their μ-TESLA secure broadcast protocol [12]. The multi-level key chain scheme uses pre-determination and broadcasting to succeed a scalable key distribution technique that is aimed to be strong toward rejection of service attacks , including jamming [8], [9]. Designed for large sensor networks, the SPINE (Secure Positioning for sensor Networks) algorithm based upon Demonstrable Multilateration. SRIL (Secure Range-Independent Localization) is designated [7]. In this paper we discover the security problems for key management for WSNs.

In this paper, we propose a Certificate less active key management to support key revocation method. The proposed method overcomes the existing limitation such as delay, threshold and energy consumption of WSNs. We use Network Simulator version is 2 (NS2) simulator to implement the proposed method. Section II describes the background information about the key management schemes. Section III discuss about the new proposed method. Finally simulation and results are discussed in Section IV.

II. RELATED WORKS

In this section, we discuss about the background information of the key management. Key management is the important construction block for all security aims in WSNs. There are several key management methods to increase the security levels.

The dynamic key management model for hierarchical heterogeneous sensor networks it is need for

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

fundamentally secure communication it is proposed by Alagheband and Aref [2]. The authors propose a dynamic key management context based on Elliptical curve cryptography (ECC) and Signcryption method for heterogeneous WSNs. The dynamic key management scheme was network scalability and sensor node (SN) movement specifically in liquescent locations. Furthermore, both broken up authentication and a fresh registering device are proposed through avoidance of SN compromise node. The dynamic key management is compared with the further seminal hierarchical heterogeneous WSN key management schemes for better in positions of communication, computation and key storage.

Sattam et al. proposed a Certificate less public key cryptography (CL-PKC), this typical used for the public key cryptography which escapes the essential escrow of identity based cryptography [14]. It does not need certificates to security the validity of public keys. The CL-PKE scheme is secure provided that an overcome the problem is closely connected to the Bilinear Diffie-Hellman Problem it is very hard.

Hsun Chuang et al. proposed a Two-layered Dynamic Key Management (TDKM) in Mobile and Long-lived Cluster-based Wireless Sensor Networks [4]. Together dynamic pair-wise key and group key management are spread in three rounds for key material exchange without encryption/decryption and exponentiation processes in TDKM. Sensor nodes (SN) are provided with some degree of properties including computation power, memory stowage, and energy. In theoretical analysis, TDKM is compared with existing key management near display its efficiency.

Huang et al. proposed a Fast Authenticated key establishment scheme, which achievements the difference in competences between security managers and sensors [5]. The hybrid scheme decreases the in elevation price public-key processes at the sensor side and exchanges them with efficient symmetric key based processes scheme. The authenticated key scheme is authenticates into the two characteristics based on public-key certificates. The public-key certificates to escape the typical key management problem in clean symmetric-key based protocols and maintain a virtuous amount of scalability. The authenticated key scheme can be professionally applied on Mitsubishi's M16C microprocessor in 5.2Kbyte code/data size, and accomplish an overall handling time of 760 MS on sensor side, which is improved than the other entire public-key based key establishment protocols we must calculated.

Wen Tao Zhu et al. proposed a Detecting node replication attacks in mobile sensor networks [16]. A wireless sensor network collected of a number of sensor nodes is often positioned in unattended and punitive atmospheres to perform several monitoring responsibilities. Unpaid to cost concerns, commonly sensor nodes are not prepared in tamper resistant, and an apprehended node may be easily compromised by an challenger. The observing applications to cripple the network and the secret credentials to discovered, the challenger can make countless duplicate nodes that are on the face of it legitimate. Detecting node replication attacks is compared with existent solutions it is better feature presentation that sensor nodes are autonomous from the breakable statement can correctly achieve their geographic locations, and that even free time organization may be in redundant.

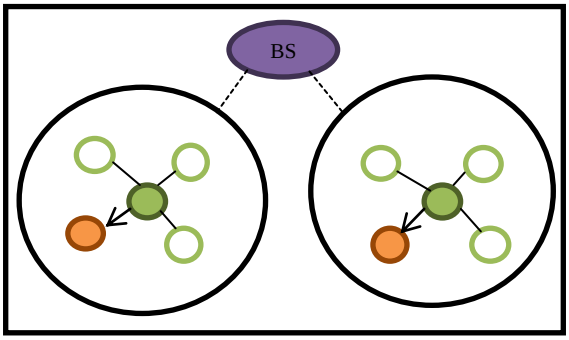
III. PROPOSED METHOD

Key management is the important construction block for all security aims in WSNs. In recent times, wireless sensor networks (WSNs) have been organized for a wide variability of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring, wherever sensory devices regularly transfer between different locations. The encryption key protocols are required to securing data and communications. In this paper, we propose a Certificate Less-Active Key Management (CL-AKM) protocol to key revocation for secure communication in dynamic WSNs and categorised by node mobility.

The proposed design is comprised of 7 phases: Structure setup, Cluster Creation, Node Movement, Key Update, Key Revocation, and Addition of a New Node.

A. Structure setup

Before the sensor nodes deployment, the Base Station (BS) creates structure parameters and registers the nodes by including it in a member listμ. The creation of nodes for our proposed key management scheme and sensor nodes are deployed over the region.



Sensor Nodes

CH - Cluster Head

BS - Base Station

CA-Update (X, Y-secret Value) – After the Node failure Key is updated to C0 and C5.

Figure 1: Proposed Scheme Structure

1) Creation of Structure Parameters: The Key Generation Centre (KGC) at the BS runs the following steps by taking a security parameter k ∈ X+ as the input, and returns a list of structure parameter.

$$\tau = \{F_i, E/F_i, G_i, P, P_{pub} = xP, h_0, h_1, h_2, h_3\}$$

DOI 10.17148/IJARCCE.2016.5129

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

- Choose a Structure Parameter τ and keeps x secret value
- Choose a k bit primer Number i
- Choose a Point Generator P
- Choose a Structure Public key of KGC $P_{pub} = xP$
- Choose cryptographic hash function $\{h_0, h_1, h_2, h_3\}$

2) Node Registration: The BS allocates a unique identifier, denoted byC_a, to each sensor node $nC_a$and a unique identifier, denoted byCH_b , to each cluster headnCH_b, where $1 \le a \le N_1, 1 \le b \le N_2, N = N_1 + N_2$.

B. Cluster Formation

Once the nodes are deployed, each cluster head through message exchanges to sensor node. Cluster head to control a cluster with the authenticated sensor node and they share a common cluster key. The cluster head also establishes a pairwise key with each member of the cluster. To simplify the discussion, we focus on the operations within one cluster and consider a^{th} the cluster. We also assume that the cluster head is n_{CH_b} with $n_{C_a}(1 \le a \le n)$ as cluster members n_{CH_b}. Establishes a cluster key for OP_b secure communication in the cluster.

C. Node Movement

Once a node moves between clusters, the cluster head requirement accurately achieved cluster keys to confirm the forward/backward confidentiality. Therefore, the cluster head updates the cluster key and informs the BS of the changed node position. Over this report, the BS can directly update the node position in the M. We denote a moving node as n_{C_m}.

1) Forward and Backward Confidentiality: CL-AKM provides the key update and revocation processes to confirm forward confidentiality as soon as a node leaves or compromised node is identified. Forward Confidentiality is an old key to continue decrypting the new messages and Backward Secrecy is a new key from backward encrypting old messages. Forward and Backward Confidentiality are used to secure against node capture attack.

2) Node Leave: A node may leave a cluster due to node failure, location change or irregular communication failure. Here be located both proactive and reactive ways for the cluster head to detect when a node leaves the cluster.

The proactive case happens as soon as the node n_{C_m}actively chooses to leave the cluster and informs the cluster head n_{CH_b}or the cluster head chooses to revoke the node. Then in this case n_{CH_b}can confirm that the node has left, it transmits a report $E_{K^0_{CH_b}}$(Node Leave, C_m) to update the BS and nC_m has left the cluster. When getting the report, the BS is updates the status of nC_m in M and sends a credit to n_{CH_b}. The reactive case happens when the cluster head n_{CH_b}fails to communicate with nC_m. It may possibly occur a node expires out of battery power, fails to connect n_{CH_b}due to interference or obstacles, is captured by the attacker or is moved unintentionally.

3) Node Join: Once the moving node nC_m leaves a cluster, it may join other clusters or return to the previous cluster after some period. We assume that nL_m wants to join the a^{th}cluster or return to the b^{th}cluster.

D. Key Update

Compromised keys and frequent encryption key updates are commonly required in directive to protect against cryptanalysis and mitigate damage. Now in this section we deliver the pairwise key update and cluster key update processes.

1) Pairwise Key Update: Only sensor nodes can update their pairwise key. Toward update a pairwise encryption key, two nodes are to shared the pairwise key perform for in a Pairwise Encryption Key Establishment process.

2) Cluster Key Update: Only cluster head can update their cluster key. If a sensor node attempts to change the cluster key, the node is considered a malicious node.

E. Key Revocation

We take responsibility that the BS can identify compromised sensors node and cluster head. The key revocation is nothing but the renewal of keys. The key revocation is calculated by the Certificate revocation list. The Certificate Revocation list split in to two categories given by old CA and New CA. The BS can require an interference detection system or malicious nodes or adversary's device to detect [13] and [17]. While we do not cover how the BS is can discover to a compromised sensor node or cluster head. In this paper, the BS can exploit the updated node position data of each cluster to explore an irregular node. Now our protocol, cluster head information is to change of its node position to the BS, when a node joins or leaves a cluster. Thus, the BS dismiss prompt achieve the node position in the member listμ. Designed for example, the BS can consider a node compromised if the node withdraws aimed at an assured period of time. Now in this case, the BS requirement explore the apprehensive node and it can be using the node error detection device introduced [6] and [10]. Once the BS discovers a compromised sensor node or a compromised cluster head is to be used in a key revocation process. A compromised node is denoted bynC_c in the b^{th} cluster for a compromise sensor node situation and a compromised head by n_{CH_b} for a compromise cluster head situation.

F. Addition of a New Node

In the past addition of a new node into present networks, adding similar data transformation to another cluster head to senor node. The BS must ensure that the sensor node is not compromised. The new node nC_{n+1}creates a full private/public key over the sensor node process stage. Before, the public structure parameters, a full private/public key and individual key$K^0_{nC_{n+1}}$are stored intonC_{n+1}.

IV. RESULTS AND DISCUSSION

We use Network simulator (NS2) to show the performance of our proposed scheme. A WSN consists of 10 sensor

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

nodes are randomly deployed over a square region of 1600 ×1600 m2 used in this simulation. The size of the data packet is 512 bytes. Adhoc on Demand Routing (AODV) protocol is used. We have 2 cluster groups. As compared to existing scheme, our proposed scheme has better performance in terms of energy consumption, delay, and throughput. The following section shows the simulation parameters, results and comparison performance of the proposed system. Table 1 shows the simulation parameters for the proposed key management method.

Simulation Parameters

Parameter	value
Field size	1600×1600 m^2
Number of sensor nodes	10
Propagation type	Two ray ground
Routing type	AODV
Packet size	512 bytes
Channel	Wireless
Simulation time	3.8 seconds

Table 1 Simulation Parameters

Performance Results

In this section, the performance of our protocol is compared with the existing method in terms of energy consumption, throughput and delay.

Fig. 2 Number of Packets vs Energy

Figure 2 shows the comparison of existing and proposed key management scheme in terms of energy. In this figure, the performance of proposed key management scheme is good energy level as compared to existing key management scheme.

Fig. 3 Number of Packets vs Threshold

Figure 3 shows the comparison of existing and proposed key management scheme in terms of Threshold. In this figure, the performance of proposed key management scheme is good threshold level as compared to existing key management scheme.

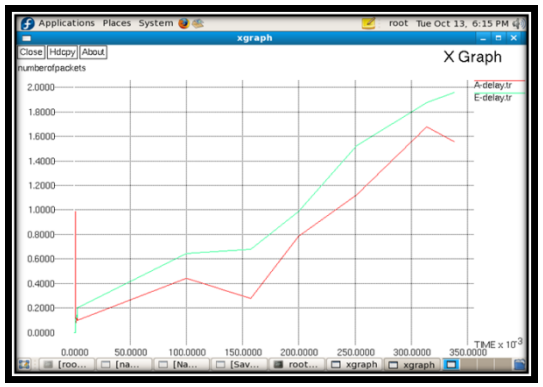


Fig. 4 Number of Packets Vs Delay

Figure 4 shows the comparison of existing and proposed key management scheme in terms of delay. In proposed key management scheme has low delay performance than the existing scheme.

V. CONCLUSION

In this paper, we propose the Certificate less Active Key Management Protocol (CL-AKM) to support effective key revocation for secure communication in dynamic WSNs. Key updated after a node movement of node leaves or node connections a cluster and key revocation for compromised nodes are supported by our proposed scheme and ensures go forward and backward key confidentiality. Our proposed scheme of security research is effective in a number of attacks and strong compared to compromise node. From the simulation results, our proposed scheme has better performance in terms of energy, throughput and delay. The investigational results establish the good organization of CL-AKM to support effective key revocation is in resource controlled WSNs.

Future work: An Anonymous Location Based Efficient Routing Protocol (ALERT). ALERT dynamically partitions the networks field into regions and randomly selects nodes in regions as intermediate relay nodes, which form a non-traceable anonymous route. Therefore, ALERT suggestions anonymity protection to sources, destination, and routes. It also has strategies to effectively counter intersection and timing attacks.

REFERENCES

[1] Akyildiz I.F., Su W., Sankarasubramaniam Y., and Cayirci E., "A Survey on Sensor Network", IEEE Communication Magazine, vol. 40, no. 8, Aug. 2002, pp. 102-114.

[2] Alagheband and Aref., "Dynamic and secure key management model for hierarchical heterogeneous sensor networks" Dept. of Electr. Eng., Sci. & Res. Branch, Islamic Azad Univ., Tehran, Iran, vol:6, issue:4.

[3] Carman D. W., Krus P. S, and Matt B. J, "Constraints and approaches for distributed sensor network security". Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[4] Hsun Chuang I., Wei-Tsung Su, Chun-Yi Wu, Jang-Pong Hsu, Yau-Hwang Kuo.,"Two-layered Dynamic Key Management in

Mobile and Long-lived Cluster-based Wireless Sensor Networks"., Dept. of Comput. Sci. & Inf. Eng., National Cheng Kung Univ., Tainan.

[5] Huang, Q.; Cukier, J.; Kobayashi, H.; Liu, B.; Zhang, J.," Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks" TR2003-102 February 2004.

[6] Jiang P., "A new method for node fault detection in wireless sensor networks," Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.

[7] Lazos L., and Poovendran R.,. "Serloc: Robust localization for wireless sensor networks". ACM Trans. Sen. Netw., 1(1):73–100, 2005.

[8] Liu, D. and Ning P. 2003. Establishing pairwise keys in distributed sensor networks. In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. ACM, New York, NY, USA, 52−61.

[9] Liu D., and Ning P., "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks". In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 263–276, 2004.

[10] Paradis L.and Han Q., "A survey of fault management in wireless sensor networks," J. Netw. Syst. Manage., vol. 15, no. 2, pp. 171–190, 2007.

[11] Perrig A., Szewczyk R., Tygar J. D., Wen V., and Culler D. E. "Spins: security protocols for sensor networks". Wireless Networking, 8(5):521–534, 2002.

[12] Perrig A., Stankovic J., and Wagner D., ―Security in Wireless Sensor Networks,‖Commun. ACM, vol. 47, no. 6, June 2004, pp. 53–57.

[13] Rassam M. A., Maarof M. A., and Zainal A., "A survey of intrusion detection schemes in wireless sensor networks," Amer. J. Appl. Sci., vol. 9, no. 10, pp. 1636–1652, 2012.

[14] Sattam S. Al-Riyami and Kenneth G. Paterson., Information Security Group," Certificateless Public Key Cryptography", Royal Holloway, University of London, Egham, Surrey, TW20 0EX.

[15] Seung-Hyun Seo., IEEE Transactions On Information Forensics And Security, Vol. 10, No. 2, February 2015.

[16] Wen Tao Zhu, Jianying Zhou, Robert H. Deng and Feng Bao., "A Detecting node replication attacks in mobile sensor networks." Vol:5, issue:5, pages 496-507, May-2012.

[17] Zhu W. T., Zhou J., Deng R. H., and Bao F., "Detecting node replication attacks in mobile sensor networks: Theory and approaches," Secur. Commun. Netw., vol. 5, no. 5, pp. 496–507, 2012.