International Journal For Technological Research In Engineering
Volume 3, Issue 10, June-2016 *ISSN (Online): 2347 - 4718*

ENTHUSIASTIC WIRELESS SENSOR NETWORKS WITH OPERATIONAL KEY FRUITION

Pulivarthi.Chandra Sekhara Satya Sai Babu[1], R.Veera Mohana Rao[2]
[1]M.Tech (CSE), Bapatla Engineering College, A.P., India
[2]Assistant Professor, Department of Computer Science & Engineering, Bapatla Engineering College, A.P., India

ABSTRACT: ***Key management has remained a difficult issue in wireless device networks (WSNs) as a consequence of the constraints of device node resources. Various key management conspiracies that trade off secrecy and operational necessities are proposed in recent years. 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 conspiracies 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. The Extend CL-EKM supports economical key updates once a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol additionally supports economical key revocation for compromised nodes and minimizes the impact of a node compromise on the protection of alternative communication links. A security analysis of our theme shows that our protocol is effective in defensive against varied attacks. we tend to implement Extended CL-EKM in Conic OS and simulate it exploitation Coola machine to assess its time, energy, communication, and memory performance.***
KEYWORDS: Wireless Sensor Networks, Key Management, and Cryptography.

I. INTRODUCTION

Wireless Sensor Network (WSN) is the network that consist of many small devices that called sensors. In literature, sometimes it is considered as a special type of the ad hoc networks [1]. These networks are useful in our life; they are widely used in many applications. WSN is used in military, commercial, and in ecological. Thus, the communications in these networks must be secure. Securing the communication in WSN is a very important issue, just because of many security threats and because of the nature of WSN. We can notice this point by studying the communication links in these networks, which is the radio links that is subject to many faulty information and malicious attacks. Sensor devices in general have a limitation in its resources; these limitations can control the nature for WSNs, also affect the security level for this type of networks. As an example for such limitations; limited processing power, battery age, transmission distance, shortage in memory space, random distribution for nodes, and bandwidth [2]. DYNAMIC wireless detector networks (WSNs), which enable quality of detector nodes, facilitate wider network coverage and additional correct service than static WSNs. Therefore, dynamic WSNs area unit being apace adopted in observance applications, like target chase in parcel of land police investigation, healthcare systems, traffic flow and vehicle standing observance, dairy cattle health observance [9]. However, detector devices are prone to malicious attacks like impersonation, interception, capture or physical destruction, because of their unattended operative environments and lapses of property in wireless communication of [20]. Thus, security is one in every of the most necessary problems in several vital dynamic WSN applications. Dynamic WSNs so ought to address key security requirements, like node authentication, knowledge confidentiality and integrity, whenever and where the nodes move. Due to the advancement of a sensing element technology, it's attainable that WSNs will contain an oversized range of inexpensive, lowpower and little sensing element nodes. There are several applications of WSNs. For instance, it includes target chase and piece of land police work in military, health care system and scientific exploration in civilian operations. The most task of WSNs is observation some sorts of space and coverage the collected knowledge to Base Station (BS) exploitation wireless channel. However it's susceptible to attacks like node capture, traffic jamming and collusion from human owing to the six characteristics of WSN [1].

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 According to the secure communication demand in WSN, 2varieties of key institution are needed. One is pair wise key institution; the opposite is cluster key institution. A few schemes has been projected that incorporates 3 phases normally [10]:(1) key setup before deployment, (2) shared-key discovery once preparation, and (3) path-key institution if 2 sensor nodes don't share an on the spot key. The most in style pair wise key pre-distribution answer is Random Pair wise Key theme [11] which addresses unessential storage drawback and provides some key resilience. It's supported Erodes and Reni's [12] work. Every sensing element node stores a

random set of Nape pair-wise keys to achieve chance p that 2 nodes are connected. Neighboring nodes will tell if they share a common pair-wise key once they send and receive"Key Discovering" Message inside radio range. Its defect is that it sacrifices key property to decrease the storage usage. Closest (location-based) pair-wise keys predistribution theme [13] is another to Random pair wise key scheme. It takes advantage of the situation data to enhance the key connectivity. Later on, Random key-chain based mostly key predistribution answer is another random key predistribution solution that originated from the answer of basic probabilistic key redistribution scheme [14]. It depends on probabilistic key sharing among the nodes of a random graph.

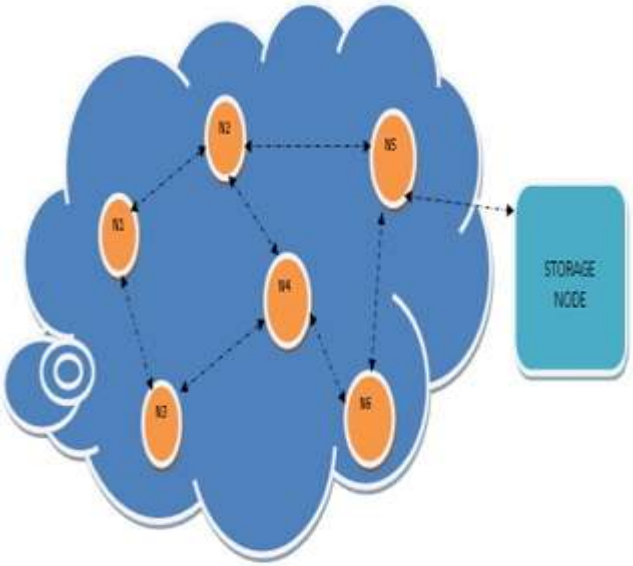

Fig 1: System Architecture

II Basic requirements and evaluation metrics Dynamic key management can be considered as a branch of key management. All key management schemes should fulfill the following traditional security requirements: confidentiality, authentication, freshness, integrity and non-repudiation. The same holds for dynamic key management schemes. In addition, according to the features and the application environment of dynamic key management, some particular evaluation measurements are highlighted. Therefore, this section de- fines the most common metrics used for evaluating dynamic key management techniques in wireless sensor networks. In [13], evaluation metrics for pre-distribution key management are classified as security, efficiency and flexibility, according to the constraints of sensor nodes and networking. Based on this classification and the unique features of dynamic key management, we present the basic requirements and evaluation metrics for dynamic key management. It has to be noted that among the following metrics, node revocation, forward and backward secrecy, collusion resistance and key connectivity are only applicable for dynamic key management schemes, while the other metrics can also be applied to static key management schemes. 2.1. Security metrics Dynamic key management schemes must provide the cryptographic keys in a secure manner, thwarting the activities of malicious nodes inside a network. Upon detecting a compromised sensor node, the current secret key of the compromised sensor node must be revoked and a new one must be generated and distributed to its associated sensor nodes, except the compromised one. Moreover, it is desirable for a dynamic key management scheme to maintain not only forward and backward secrecy, but also collusion resistance between the newly joined nodes and the compromised ones. In addition, resilience against node capture and node replication needs to be provided. 1. Node revocation. Once compromised sensor nodes are detected, an effective solution should be able to revoke them promptly from the network. Such mechanisms are useful to prevent a compromised node from deviating the network behavior by injecting false data or modifying data of trusted nodes. 2. Forward and backward secrecy. Forward secrecy is used to prevent a node from using an old key to continue decrypting new messages [20]. Backward secrecy is the opposite, it is used to prevent a node with the new key from going backwards in time to decipher previously received messages encrypted with prior keys [20]. Both forward and backward secrecy are used to defeat node capture attacks. 3. Collusion resistance. An adversary might attack the network by compromising a number of nodes in the network, making these nodes collude and collaboratively reveal all system keys and consequently capture the entire network. A good dynamic key establishment technique must resist the collusion of newly joined and compromised nodes. 4. Resilience. Resilience indicates the resistance against node capture, where the adversary physically attacks a sensor node and tries to recover secret information from its memory. It measures the impact of one captured node on the rest of the network. The resilience of a key management system is high if an adversary cannot affect any node except the captured one. In contrast, the resilience is low if the capture of a single node leads to the compromise of the whole network.

III. SYSTEM MODEL

In the present work we consider the DTN environment without any centralized trusted authority (TA). Nodes are able to use multi hops communication. Node exchanges the information on encounters with another node.

Selfish Behavior and Model

The selfish behavior of the node is defined as the unwillingness of node in participation of its resources on others requirement, this is generally done to maintain its limited resources such as power. Since DTNs required participation of all nodes in packet relaying this could cause severe degradation of the performance. They considered selfish nodes acts for its own interests, so to save energy it just drop the packet but it may decide to forward a message with a certain probability. Two kind of selfishness: 1. Individual Selfishness: Here node forwards only those packets which are generated by it and drop packets from other node. 2. Social Selfishness: Here nodes are willing to forward packets for other nodes with

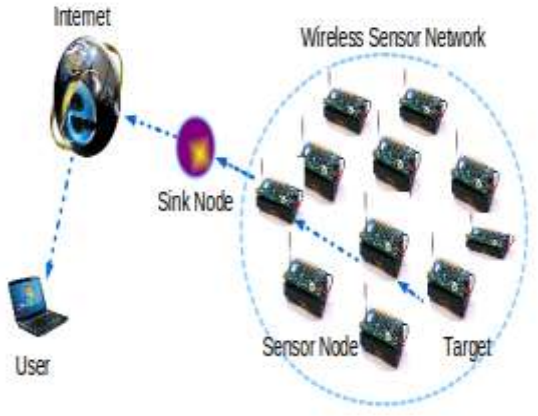

Fig 2: System model

whom they have social connect but not others and such willingness varies with the strength. Strategies [13] for prevention of selfishness are as follows: 1. Barter Based 2. Credit Based 3. Reputation Based. Barter Based is pair wise Tit-For-Tat strategy. The procedure is that two encounter nodes exchange the equal value of messages. A message in which the nodes are interested is called primary message and other are secondary messages, hence it degrades the performance of nodes drastically. Credit Based strategy are cooperative to forward the messages, the idea is to get certain amount of credit as a reward that it can later explore for its own profit. Credit Based are generally of two types: Message Purse Model and Message Trade Model. In Message Purse Model source node pay credits to the intermediate nodes which are involve in forward the messages to the destination. In Message Trade Model the sender of the message pay credits to receivers in each hop-by-hop transmission until the message reach the destination, which finally pays credits for the message forwarding. Reputation Based strategy based upon cooperative experiences and observation of its past activities. If the reputation value of a node is less, it reflects that the node is selfish according to other nodes, otherwise Cooperative nature to the nodes. Each intermediate node receives a reputation value after pass a message to other nodes. The reputation value is a proof about the cooperative nature of the intermediate node. Reputation Based are generally of two types: Detection Based Model and Without Detection Based Model. In Detection Based every node detects the behaviour of the receiver which receives the message from him, in order to monitor the selfishness and encourage them to be cooperative in nature. In reputation the node is punished if it is not cooperate in nature. Reputation is also used in Social Selfishness Aware Routing (SSAR), the performance of the node is not affected by the not well-behaved nodes. First check the willingness of receiving node if it is ready then the message with higher delivery probability in the network is transferred. When a node behave as a selfish then forward the messages only to its community while a malicious node aims to break all the protocols of basic DTN routing functionality. A malicious node drops the packets and also performs the trust related attacks: 1. Self-promoting attacks: To attract other packets in the network its increase own importance by providing good credits or recommendations for itself. 2. Bad-monitoring attacks: It decreases the probability of packet routing through good nodes by providing bad recommendations and its ruin the reputation of well-behaved nodes. 3. Ballot stuffing: It increase the probability of packet transfer through malicious node by proving good recommendations to the bad nodes, it increase the reputation of not well-behaved nodes. A malicious node attacker performs random attacks to evade detection. We introduce a new random attack probability to reflect random attack behavior. When random attack probability is equal to 1, the malicious attacker is a reckless attacker, when random attack probability is less than 1 it is a random attacker. The node trust value is directly accessed by the trust evaluation and indirect trust value by recommendations.

IV. PROPOSED SCHEME

In this paper, we present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs. In certificateless public key cryptography (CL-PKC), the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key. We also take the benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length.In order to dynamically provide both node authentication and establish a *pairwise key* between nodes, we build CL-EKM by utilizing a pairing-free certificateless hybrid signcryption scheme (CL-HSC).

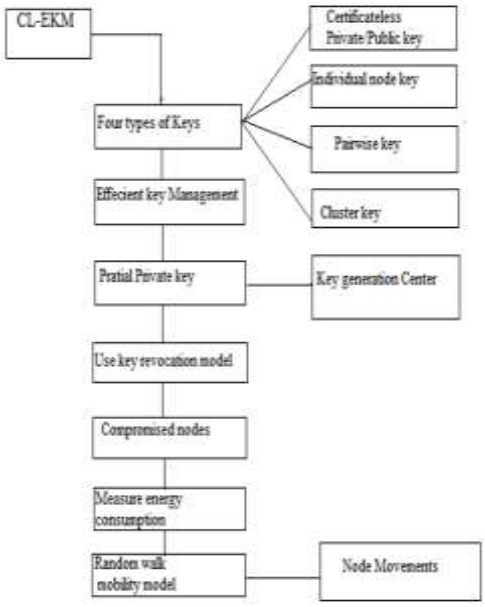

Fig: flow of proposed system

ADVANTAGES OF PROPOSED SYSTEM:

To support node mobility, our CL-EKM also supports lightweight processes for cluster key updates executed when a node moves, and key revocation is executed when a node is detected as malicious or leaves the cluster permanently.

CL-EKM is scalable in case of additions of new nodes after network deployment. CL-EKM is secure against node compromise, cloning and impersonation, and ensures forward and backward secrecy. The security analysis of our scheme shows its effectiveness.

V. OVERVIEW OF THE CERTIFICATELESS EFFECTIVE KEY MANAGEMENTAND SECURITY MODEL SCHEME KEY MANAGEMENT

Before WSN will exchange information firmly, encryption keys should be established among sensing element nodes. Key distribution refers to the distribution of multiple keys among the sensing element nodes, which is typical in an exceedingly non-trivial security theme. Key management could be a broader terms for key distribution, which conjointly includes the processes of key setup, the initial distribution of keys, and key revocation — the removal of a compromised key. A. Network Model We contemplate a heterogeneous dynamic wireless device network (See Fig. 1). The network consists of variety of stationary or mobile device nodes and a bachelor's degree that manages the network and collects knowledge from the sensors. Device nodes will be of 2 types: (i) nodes with high process capabilities, referred to as H-sensors, and (ii) nodes with low process capabilities, said as Lsensors. We have a tendency to assume to own N nodes within the network with variety N1 of H-sensors and variety N2 of Lsensors, wherever N = N1 + N2, and N1 N2. Nodes could be part of and leave the network, and thus the network size could dynamically amendment. The H-sensors act as cluster heads whereas L-sensors act as cluster members. They are connected to the bachelor's degree directly or by a multi-hop path through other H-sensors. H-sensors and Lsensors will be stationary or mobile. Once the network preparation, every H-sensor forms a cluster by discovering the neighboring Lsensors through beacon message exchanges. The L-sensors will be part of a cluster, move to different clusters and conjointly re-join the previous clusters. To maintain the updated list of neighbors and property, the nodes in an

VI. CONCLUSION

This Project proposed to the primary certificate less effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CLEKM support economical communication for key updates and management once a node leaves or joins a cluster and thence ensures forward and backward key secrecy. Our theme is resilient against node compromise, cloning and impersonation attacks and protects the info confidentiality and integrity. This project have a tendency to introduce a replacement theme which will be used for establish varied keys (pair wise keys, path keys and cluster keys) for wireless device networks. It is able to do quick credibility while not further computations and communications. The experiment result shows the performance of TKLU is fresh. Associate in nursing energy-efficient dynamic key management theme victimization the EBSs, polynomials and secret symmetry keys. EEDKM provides localized rekeying which is effectively performed not poignant the opposite elements of WSN. Since EEDKM uses bilaterally symmetric key between the bachelor's degree and sensor node, it will certify the node and performs rekeying more energy expeditiously than LOCK within the higher layer. EEDKM is additional resilient than general key management scheme supported the EBSs and polynomial keys. Therefore rekeying is performed less of times. These mathematical models are utilized to estimate the right worth for the Told and Takeoff for parameters supported the speed and also the desired exchange between the energy consumption and also the security level.

REFERENCES

[1] Jongho Won ; Salmin Sultana ; Elisa Bertino, "Effective Key Management in Dynamic Wireless Sensor NetworksIEEE Transactions on Information Forensics and Security Feb. 2015

[2] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key redistribution scheme for sensor networks using deployment knowledge," IEEE Trans. Dependable Secure Compute., vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.

[3] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Kaila, "A pair wise key redistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.

[4] M. Rah man and K. El-Katie, "Private Key agreement and secure communication for heterogeneous sensor networks," J. Parallel Diatribe. Compute. vol. 70, no. 8, pp. 858–870, 2010.

[5] M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Inf. Secure., vol. 6, no. 4, pp. 271–280, Dec. 2012

[6] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz.(2005) Energy Analysis of Public Key Cryptography for Wireless Sensor Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324– 328.

[7] M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic Key Management in Sensor Networks," Communications Magazine, IEEE, vol 44, pp 122-130, April 2006

[8] B.B. Chen and M.C. Chan, "Mobicent: A Credit-BasedIncentive System for Disruption-Tolerant Network," Proc. IEEEINFOCOM'10,2010.

[9] A. Lindgren and A. Doria, "Probabilistic Routing Protocol for Intermittently Connected Networks," draft-lindgren-dtnrgprophet-03, 2007.

[10] W. Gao and G. Cao, "User-Centric Data

Dissemination in Disruption Tolerant Networks," Proc. IEEE INFOCOM '11, 2011.
[11] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.
[12] O. Younis, M. Krunz, and S. Ramasubramanian, "NodeClusteringinWirelessSensorNetworks:Recent DevelopmentsandDeploymentChallenges,"IEEENetwork, vol.20,no.3,pp.20-25,May/June2006.
[13] S. Bandyopadhyay and E. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," Proc.IEEE INFOCOM, vol. 3, pp. 1713-1723, Mar.2003.
[14] Vahdat, Amin; Becker, David (2000), "Epidemic routing for partially connected ad hoc networks", Technical Report CS-2000- 06, Duke University.
[15] Harminder Singh Bindra, AmritLalSangal," Considerations and Open Issues in Delay Tolerant Network'S (DTNs) Security", Department of Computer Science and Engineering, NIT Jalandhar, Punjab, India, June 2, 2010.

AUTHORS:

Pulivarthi.chandra sekhara satya sai babu received B.Tech from khader memorial college ofEngineeringand Technology, Devarakonda, from JNTU Hyderabad, A.P, India. Presently, He pursuingM.Tech in C.S.E fromBapatla Engineering College the specialization in Computer Science & Engineering.

R.Veera Mohana Rao received B.Tech in IT from St.Ann's college of engineering and technology, from JNTUK,A.P., India. M.Tech in C.S.E from Vignan University, A.P., India. He has published papers in international journals and national conferences in the area of wireless sensor networks, computer networks, network security and is currently working as Assistant Professor in Dept of CSE, Bapatla Engineering College, Bapatla, A.P., India.

