ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Securing Data and Communications Key Management in Dynamic Wireless Sensor Network

Dr.Shaik Abdul Nabi
Professor,
Dept of CSE,
AVN Institute of Engineering and Technology.

G.Dayakar
Assistant Professor,
Dept of CSE,
AVN Institute of Engineering and Technology.

P.Ramesh
PG Scholar,
Dept of CSE,
AVN Institute of Engineering and Technology.

Abstract:

Key management has remained a difficult issue in wireless device networks (WSNs) as a result of the constraints of device node resources. Various key management schemes that trade off security and operational necessities are proposed in recent years. Wireless device Networks (WSNs) comprises tiny sensor nodes with strained energy, memory and computation capabilities. They're typically deployed within the unattended and hostile environment. So device nodes area unit susceptible to attacks such as node capture and collusion attack by adverseries. This paper proposes a key distribution theme, based on Exclusion-based systems (EBSs) and tdegree quantity. Its associate degree energyefficient dynamic key management scheme that performs localized rekeying to reduce overhead.

In this paper, we tend to propose a certificate less-effective key management (CLEKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The 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 CL-EKM in Conic OS and simulate it exploitation Coola machine to assess its time, energy, communication, and memory performance.

I.INTRODUCTION:

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, low power 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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]. These six characteristics are shown below. terribly massive and dense WSN • Lack of mounted infrastructure • Unknown topology before preparation • High risk of physical attacks to unattended sensors. In order to dynamically give each node authentication and establish a pair wise key between nodes, we build CL-EKM by utilizing a pairing-free certificate less hybrid signcryption theme (CL-HSC) planned by America in AN earlier work [13], [14]. as a result of the properties of CL-HSC, the pair wise key of CL-EKM will be with efficiency shared between two nodes while not requiring onerous pairing operations and the exchange of certificates. To support node quality, our CL-EKM additionally supports light-weight processes for cluster key updates dead once a node moves, and key revocation is executed once a node is detected as malicious or leaves the cluster for good.

CL-EKM is scalable just in case of additives of new nodes once network preparation. CL-EKM is secure against node compromise, biological research and impersonation, and ensures forward and backward secrecy. The safety analysis of our theme shows its effectiveness. Below we tend to summarize the contributions of this paper: • we tend to show the safety weaknesses of existing ECC based mostly key management schemes for dynamic WSNs. • we tend to propose the primary certificate less effective key management theme (CL-EKM) for dynamic WSNs. CL-EKM supports four sorts of keys, every of that is used for a special purpose, as well as secure pair-wise node communication and group-oriented key communication among clusters. Economical key management procedures area unit outlined as supporting node movements across completely different clusters and key revocation method for compromised nodes.

CL-EKM is enforced mistreatment Contiki OS and use a TI exp5438 ape to live the computation and communication overhead of CL EKM. Additionally we tend to develop a machine to live the energy consumption of CL-EKM. Then, we tend to conduct the simulation of node movement by adopting the stochastic process quality Model and the Manhattan quality Model among the grid. The experimental results show that our CL-EKM theme is lightweight and thence appropriate for dynamic WSNs. In Section a pair of, we tend to shortly discuss connected work and show the security weaknesses of the present schemes. As WSNs are developed, the additional WSNs are developed, the more it becomes advanced and dynamic. So there's a need to use dynamic key management theme which will amendment the administrative keys by amount and on demand or upon detection of node capture. This theme enhances the network survivability.

The foremost concern of dynamic keying may be a designing the rekeying mechanism. EBS [6] is one amongst the representative solutions. However, there's a haul that a small variety of nodes could conspire and reveal the entire network keys. to boost the fundamental Ebbs' answer, SHELL uses the post-deployment location info. However, it is inefficient; as a result of SHELL rely upon the centralized key server. Recently another increased Ebbs scheme-LOCK [8] was proposed. It uses 2 layers of Ebbs body keys and t-degree quantity polynomials. This paper additionally proposes new key management theme based on Ebbs and t-degree quantity polynomials. By using secret keys between the baccalaureate and cluster heads, this theme could bring additional energy-efficient results than LOCK. The remainder of this paper is organized as follows. Section a pair of overviews the fundamental WSN model and analysis metrics. Section three explains the background techniques merely.

II. Related work

According to the secure communication demand in WSN, 2varieties of key institution are needed.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. There are many key reinforcement proposals to strengthen security of the established link keys, and improve resilience. Objective is to firmly generate a novel link or path key by using established keys, so the secret's not com-secure once one or a lot of sensing element node is captured. One approach is to extend quantity of key overlap needed in shared key discovery phase. Q-composite random key pre distribution theme [11] needs letter common keys to establish a link key. Similar mechanism is projected by Pair-wise key institution protocol [15] that uses threshold secret sharing for key reinforcement. The key reinforcement solutions in general increase process and communication quality; however give smart resilience in the sense that compromised key-chain doesn't directly have an effect on security of any links within the WSN.

But, it should be doable for Associate in Nursing oppose to re- cowl initial link keys. Associate in Nursing oppose will then recover strengthened link keys from the recorded multi-path reinforcement messages once the link keys are compromised. Symmetric key schemes don't seem to be viable for mobile detector nodes and so past approaches have targeted solely on static WSNs. a couple of approaches are planned supported PKC to support dynamic WSNs. Thus, during this section, we review previous PKC-based key management schemes for dynamicWSNs and analyze their security weaknesses or disadvantages. Chuang et al. [7] and Agawam et al. [8] planned a two-layered key management theme and a dynamic key update protocol in dynamic WSNs supported the DaffierHellman (DH), severally. However, both schemes don't seem to be fitted to sensors with restricted resources and area unit unable to perform valuable computations with massive key sizes (e.g. a minimum of 1024 bit).

Since computer code is computationally additiona l economical and features a short key length (e.g. 160 bit), many approaches with certificate are planned supported computer code. However, since every node should exchange the certificate to ascertain the pair wise key and verify every other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes don't seem to be secure. Alagheband et al. [5] planned a key management theme by victimization ECCbased signcryption, but this theme is insecure against message forgery attacks [16].Huang et al. [15] planned a ECC-based key institution scheme for self-organizing WSNs. However, we tend to found the security weaknesses of their theme. In step a pair of of their theme, a detector node U sends z = qU · H (Mackey) + dU (mown) to the opposite node V for authentication, wherever qU may be a static personal key of U. But, once V receives the z, it can disclose qU, as a result of V already got Mackey and dU in step one. So, V will simply acquire qU by computing qU = (z − dU) · H(Mackey) −1.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Thus, the detector node's private secret is exposed to the opposite node throughout the key establishment between 2 nodes. Zhang et al. [10] planned a distributed settled key management theme supportedECC for dynamic WSNs. It uses the isosceles key approach for sharing the pair wise key for existing nodes and uses an asymmetric key approach to share the pair wise keys for a new node when readying. However, since the initial key KI is used to figure the individual keys and also the pair wise keys after readying for all nodes, if a soul obtains KI, the adversary has the flexibility to figure all individual keys and the pair wise keys for all nodes. Thus, such theme suffers from weak resilience to node compromises. Also, since such theme uses a straightforward ECC-based DH key agreement by victimization every node's semipermant public key and personal key, the shared pair wise secret is static and as a result, is not secure against known-key attacks and can't give re-key operation use a ECDSA theme to verify the identity of a cluster head and a static EC-DiffieHellman key agreement theme to share the pair wise key between the cluster heads.

Therefore, the theme by Duet al. isn't secure against known-key attacks, as a result of the pair wise key between the cluster heads is static. On the opposite hand, Du et al. use a standard arithmetic-based isosceles key approach to share the pair wise key between a detector node and a cluster head. Thus, a detector node cannot directly establish a pair wise key with different detector nodes and, instead, it needs the support of the cluster head. In their theme, in order to ascertain a pair wise key between two nodes within the same cluster, the cluster head arbitrarily generates a pair wise key and encrypts it victimization the shared keys with these two nodes. Then the cluster head transmits the encrypted pairwise key to every node. Thus, if the cluster head is compromised, the pair wise keys between non-compromised detector nodes in the same cluster will be compromised.

III. SYSTEM MODEL& ANALYSIS METRICS

A. System Model

The basic system model of this paper is pictured in Figure.1.It consists of 1 BS and lots of uniform sensing element nodes with distinctive ID. It uses cluster and two-layer design for scalability. Every cluster has some key generation nodes (KGNs) that distribute point keys among that cluster. These KGNs is also the final sensing element nodes elect by cluster heads (CHs).We assume that the fundamental system model is deployed for the purpose of watching the hostile atmosphere. End-to-end node communication is unusual as a result of sensing element nodes in each cluster monitor the finite space. For the info aggregation, there square measure several communications between the nodes among the same cluster. Thus, the most task of this model could be a information transfer from sensing element nodes to BS and an information aggregation in every cluster...

B. ANALYSIS METRICS

WSNs have some criteria that represent fascinating characteristics in key management scheme. To boot, energy consumption is that the most vital criterion thanks to the power constraint of detector nodes. Energy consumption might affect primarily the network lifespan. The key criteria square measure shown below.

- Resilience against node capture
- Revocation
- Scale
- Energy consumption

IV. PROPOSED SCHEME

This paper introduces an Energy-Efficient Dynamic Key Management (EEDKM) proposal that uses two-layer architecture. In the lower layer, similar to LOCK, rekeying is performed confined using the EBS and the t-degree vicariate polynomial. Each cluster has a clear number of KGNs which makes it hard that an attacker can exposes the network keys by obtaining some KGNs. In upper layer, rekeying is performed using the secret key between BS and sensor node. The secret key is loaded before in each sensor node with unique ID and authenticates the node to the BS.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The BS generates one t-degree vicariate polynomial key and distributes it by means of session key shared by all CHs. This makes the communication between CHs efficient. The rest of this section describes the bootstrapping, initial key distribution mechanism and some general operations in our key management scheme. This may help you to understand our scheme.

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 exceedingly cluster sporadically exchange very light-weight beacon messages. The H-sensors report any changes in their clusters to the bachelor's degree, as an example, once an Lsensor leaves or joins the cluster. The bachelor's degree creates a listing of legitimate nodes; Associate in Nursing updates the standing of the nodes once an anomaly node or node failure is detected. The bachelor's degree assigns every node a unique symbol. A L-sensor nil is unambiguously known by node ID Li whereas a H-sensor nHj is assigned a node ID Hj . A Key Generation Center (KGC), hosted at the bachelor's degree, generates public system parameters used for key management by the BS and problems certificate less public/private key pairs for every node within the network. In our key management system, a unique individual key, shared solely between the node and also the bachelor's degree is assigned to every node. The certificate less public/private key of a node is employed to ascertain pair wise keys between any 2 nodes. A cluster secret's shared among the nodes in a very cluster

B. Adversary Model and Security Requirements

We assume that someone will mount a physical attack on a device node once the node is deployed and retrieve secret information and knowledge keep within the node.The someone also can populate the network with the clones of the captured node. Even while not capturing a node, Associate in nursing someone will conduct Associate in nursing impersonation attack by injecting Associate in nursing illegitimate node, which attempts to impersonate a legitimate node. Adversaries will conduct passive attacks, such as, eavesdropping, replay attack, etc to compromise knowledge confidentiality and integrity. Specific to our planned key management theme, if someone perform a known-key attack to be told pair wise master keys if it somehow learns the short keys, e.g., pair wise secret writing keys.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

VI.CONCLUSION

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] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Sump. SP, May 2003, pp. 197–213.

[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.

Author's Details:

Dr. Shaik Abdul Nabi is working as professor & Head of the Dept. of CSE, AVN Inst.Of Engg.& Tech, Hyderabad, T.S, India. He completed his B.E (Computer Science) from Osmania University, Hyderabad. He has completed his M.Tech. from JNTU Hyderabad campus and he received Doctor of Philosophy (Ph.D) in the area of Web Mining from AcharyaNagarjuna University, Guntur, AP, India. He is a certified professional by Microsoft.He is having 17 years of Teaching Experience in various Engineering Colleges. He has published 15 publications in International / National Journals and presented 08 papers in National / International conferences. His expertise areas are Data warehousing and Data Mining, Data Structures & UNIX Networking Programming, Cloud Computing and Mobile Computing

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

G.Dayakar is working as Asst. Professor in Dept. of CSE, AVN Institute Of Engineering & Technology, Hyderabad, T.S, India. He completed his B.Tech (Computer Science) from JNTU, Hyderabad. He has completed his M.Tech. from JNTU Hyderabad campus, India. He is a certified professional in Teaching by National Institute Of Technical Teachers Training & Research (Govt Of India) He is having 10 years of Teaching Experience in various Engineering Colleges. His expertise areas are Design and Analysis Of Algortithms, Data Structures & UNIX Networking Programming.

P.Ramesh PG Scholar in Dept of CSE .AVN Institute of Engineering And Technology