Dynamic improved key Management and security in WSN

D Venu Gopal Nair[1], Sana khanam [2]

[1] *Assoc Prof, CSE Dept, Institute of Engineering and Technology, Lucknow .*

[2] *PG Scholar, Dept of CSE, Institute of Engineering and Technology, Lucknow.*

Abstract:-

In recent years, wireless sensing element networks (WSNs) are deployed for a large type of applications, including military sensing and trailing, patient standing observance, traffic flow observance, wherever sensory devices typically move between different locations. Securing information and communications needs appropriate encoding key protocols. During this paper, we propose a certificate less effective key management protocol (CL-EKM) for secure communication in dynamic wireless sensing element networks characterized by node quality. 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 different communication links. A security analysis of our theme shows that our protocol is effective in defensive against varied attacks. we have a tendency to implement CL-EKM in Contiki OS and simulate it exploitation Cooja machine to assess its time, energy, communication and memory performance.

Index Terms—Wireless sensor networks, certificate less public key cryptography, key management scheme

I.INTRODUCTION:- Dynamic wireless device networks (WSNs), that change mobility of device nodes, facilitate wider network coverage and a lot of correct service than static WSNs. Therefore, dynamic WSNs square measure being quickly adopted in observation applications, like target following in tract police investigation, care systems, traffic flow and vehicle standing observation, dairy cow health observation [9]. However, device devices square measure vulnerable to malicious attacks like impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of property in wireless communication [20]. Thus, security is one among the foremost necessary problems in several essential dynamic WSN applications. Dynamic WSNs so have to be compelled to address key security necessities, such as node authentication, information confidentiality and integrity, whenever and where the nodes move. To address security, coding key management protocols for dynamic WSNs are projected

in the past supported symmetrical key coding [1], [2], [3]. Such form of coding is well-suited for sensor nodes owing to their restricted energy and processing capability. However, it suffers from high communication overhead and needs giant memory, space to store shared pair wise keys. it's conjointly not scalable and not resilient against compromises, and unable to support node quality. Thus satellite key encoding isn't appropriate for dynamic WSNs. More recently, uneven key based mostly approaches have been projected for dynamic WSNs [4], [5]. These approaches cash in of public key cryptography (PKC) like elliptic curve cryptography (ECC) or identity-based public key cryptography (ID-PKC) so as to alter key establishment and knowledge authentication between nodes. PKC is comparatively dearer than satellite key encoding with relevancy process prices. However, recent enhancements within the implementation of computer code [11] have incontestable the practicability of applying PKC to WSNs. for example, the implementation of 160-bit computer code on associate Atmel AT-mega 128, which has associate eight-bit 8 MHz CPU, shows that associate computer code point multiplication takes but one second [11]. Moreover, PKC is a lot of resilient to node compromise attacks and is a lot of climbable and versatile. However, we found the protection we have a tendency tokenizes of existing ECC based schemes [5] that these approaches are at risk of message forgery, key compromise and known-key attacks. Also, we have a tendency to analyze the crucial

security flaws of that the static personal secret's exposed to the opposite once each nodes establish the session key. Moreover, these ECC-based schemes with certificates once directly applied to dynamic WSNs, suffer from the certificate management overhead of all the device nodes then don't seem to be a use for large scale WSNs. The pairing operation-based ID-PKC [4] schemes area unit inefficient owing to the computational overhead for pairing operations. To the best of our data, economical and secure key, management schemes for dynamic WSNs have not yet been proposed.

In this paper, we have a tendency to gift a certificate less effective key management (CL-EKM) theme for dynamic WSNs. In certificate less public key cryptography (CLPKC) [12], the user's full non-public secret's a mixture of a partial non-public key generated by a key generation center (KGC) and therefore the user's own secret worth. The special organization of the total private/public key try removes the necessity for certificates and additionally resolves the key written agreement downside by removing the responsibility for the user's full non-public key. we have a tendency to additionally take the profit of ECC keys outlined on Associate in Nursing additive cluster with a 160- bit length as secure because the RSA keys with 1024-bitlength.

In this so as 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 U.S.A. in Associate in Nursing earlier work [13]. Due to the properties of CL-HSC, the pair wise key of CLEKM can be expeditiously shared between 2 nodes without requiring heavy pairing operations and therefore the exchange of certificates. To support node quality, our CL-EKM conjointly supports light-weight processes for cluster key updates dead once a node moves, and key revocation is dead once a node is detected as malicious or leaves the cluster for good. CLEKM is climbable just in case of additives of recent nodes after 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 summarize the contributions of this paper:

II.IMPORTANT POINTS:-

1. We show the security weaknesses of existing ECC based key management schemes for dynamic WSNs [10]].
1. We propose the first certificate less effective key management scheme (CL-EKM) for dynamic WSNs. CL-EKM supports four types of keys, each of which is used for a different purpose, including secure pair-wise node communication and group-oriented key communication within clusters. Efficient key management procedures are defined as supporting node movements across different clusters and key revocation process for compromised nodes.
2. 3 CL-EKM is implemented using Contac OS and use a TI exp5438 emulator to measure the computation and communication overhead of CLEKM. Also we develop a simulator to measure the energy consumption of CL-EKM. Then, we conduct the simulation of node movement by adopting the Random Walk Mobility Model and the Manhattan Mobility Model within the grid.

III. RELATED WORK:-

Symmetric key schemes don't seem to be viable for mobile sensor nodes and so past approaches have targeted only on static WSNs. a couple of approaches are proposed supported PKC to support dynamic WSNs. Thus, during this section, we have a tendency to review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al. [7] and Agrawal et al. [27] planned a two-layered key management theme and a dynamic key update protocol in dynamic WSNs based mostly on the Diffie-Hellman (DH), severally. However, both schemes [7], [27] don't seem to be fitted to sensors with limited resources and are unable to perform expensive computations with giant key sizes (e.g. at least1024 bit). Since error correction code is computationally additional economical and includes a short key length (e.g. 160 bit), several approaches with certificate [5] have been planned supported error correction code. However, since each node should exchange the certificate to determine the pair wise key and verify every other's certificate before use, the communication and computation overhead increase dramatically. Also, the bachelor's degree suffers from the overhead of certificate management. Moreover,

existing schemes [15] don't seem to be secure. Algae bandit al. [5] projected a key management theme by mistreatment ECC-based signcryption, however this theme is insecure against message forgery attacks [16]. Huang et al. [15] projected a ECC-based key institution scheme for self-organizing WSNs. However, we found the security weaknesses of their scheme. In step 2of their scheme, a sensor node U sends z = qU _H(Mackey) + dU(modn) to the other node V for authentication, where qU is a static private key of U. But, once V receives the z, it can disclose qU, because V already got MacKey and dU in step 1.So, V can easily obtain qU by computing qU = (z □dU) _ H(MacKey)□1. Thus, the sensor node's private key is exposed to the other node during the key establishment between two nodes. However, since the initial key KI is used to reckon the individual keys and also the pair wise keys when preparation for all nodes, if AN resister obtains KI , the resister has the power to reckon all individual keys and also the pair wise keys for all nodes. Thus, such theme suffers from weak resilience to node compromises. Also, since such theme uses a simple ECC-based DH key agreement by victimization every node's long-run 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 offer re-key operation. Du et al. [25] use a ECDSA theme to verify the identity of a cluster head and a static EC-Diffie-Hellman key agreement theme to share the pair wise key between the cluster heads. Therefore, the scheme by Du et 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 modular arithmetic-based even key approach to share the pair wise key between a detector node and a cluster head. Thus, a device node cannot directly establish a pair wise key with alternative device nodes and, instead, it needs the support of the cluster head. In their theme, so as to determine a pair wise key between two nodes within the same cluster, the cluster head randomly generates a pair wise key and encrypts it using the shared keys with these 2 nodes. Then the cluster head transmits the encrypted pair wise key to each node. Thus, if the cluster head is compromised,
the pair wise keys between non-compromised device nodes within the same cluster will be compromised. Therefore, their theme isn't compromise-resilient against cluster head capture, as a result of the cluster head randomly generates a pair wise key between device nodes whenever it's requested by the nodes. Moreover, in their theme, so as to share a pair wise key between 2 nodes in numerous clusters, these two nodes should communicate via their several cluster heads. So, once one cluster head generates the pair wise key for 2 nodes, the cluster head should firmly transmit this key to each its node and also the alternative cluster head. Thus, this pair wise key ought to be encrypted by using the shared pair wise key with the opposite cluster head and also the shared key with its node, severally. Therefore, if the pair wise key between the cluster heads is exposed, all pair wise keys of the 2 nodes in different clusters square measure disclosed. The theme by Du et al. supports forward and backward secrecy by mistreatment a key update method whenever a brand new node joins the cluster or if a node is compromised. However, the scheme doesn't give a method to safeguard against clone and impersonation attack.

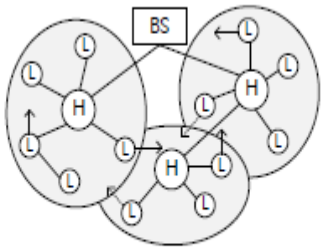


Fig. 1. Heterogeneous dynamic wireless sensor network

Adversary Model and Security Requirements:-

We assume that the mortal will mount a physical attack on a sensing element node once the node is deployed and retrieve secret data and knowledge hold on within the node. The mortal also can populate the network with the clones of the captured node. Even while not capturing a node, AN mortal will conduct AN impersonation attack by injecting AN illegitimate node, which makes an attempt 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, the mortal will perform a known-key attack to find out pair wise master keys if it somehow learns the short-run keys, e.g., pair wise encryption keys. As delineate in [7], so as to provide a secure key management

theme for WSNs supporting mobile nodes, the subsequent security properties are critical:

1. Compromise-resilience: A compromised node must not affect the security of the keys of other legitimate nodes. In other words, the compromised node must not be able to reveal pair wise keys of non-compromised nodes. The compromise resilience definition does not mean that a node is resilient against capture attacks or that a captured node is prevented from sending false data to other nodes, BS, or cluster heads.
2. Resistance against cloning and impersonation: The scheme must support node authentication to protect against node replication and impersonation attacks.
3. Forward and backward secrecy: The scheme must assure forward secrecy to prevent a node from using an old key to continue decrypting new messages. It must also assure backward secrecy to prevent a node with the new key from going backwards in time to decrypt previously exchanged messages encrypted with prior keys. Forward and backward secrecy are used to protect against node capture attacks.

Types of keys:

Pair wise key: every node shares a unique pair wise key with every of its neighboring nodes for secure communications and authentication of these nodes. as an example, so as to hitch a cluster, a L-sensor ought to share a pair wise key with the H-sensor. Then, the H-sensor will securely cipher and distribute its cluster key to the L-sensor by victimization the pair wise key.

In aggregation collateral WSN, the L-sensor can use its pair wise key to firmly transmit the perceived knowledge to the H-sensor. Every node will dynamically establish the pair wise key between itself and another node victimization their various certificate less public/private key pairs.

Cluster key: All nodes during a cluster share a key, named as cluster key. The cluster key's in the main used for securing broadcast messages during a cluster, e.g., sensitive commands or the amendment of member status during a cluster. Solely the cluster head will update the cluster key once a L-sensor leaves or joins the cluster.

Certificate less Public/Private Key: Before a node is deployed, the KGC at the bachelor's degree generates a singular certificate less private/public key try and installs the keys within the node. This key try is employed to generate a reciprocally genuine pair wise key.

Individual Node Key: every node shares a singular individual key with bachelor's degree. As an example, an L-sensor can use the individual key to cipher associate alert message sent to the bachelor's degree, or if it fails to speak with the H-sensor. Associate H-sensor will use its individual key to cipher the message corresponding to changes within the cluster. The BS can also use this key to cipher any sensitive data, like compromised node data or commands. Before a node is deployed, the BS assigns the node the individual key.

TABLE 1
List of Notations

L_i	Unique identifier of an L-sensor node n_{L_i}
H_j	Unique identifier of an H-sensor node n_{H_j}
ID_{BS}	Identifier of the Base Station (BS)
q	A k bit primer number
P_{pub}	A system public key of KGC, $P_{pub} = xP$
x	A master private key of KGC
P	Point generator of an additive cyclic group G_q
$\mathbb{Z}^*_q$	The multiplicative group of integers modulo q
E/F_q	The selected elliptic curve over the field F_q: $y^2 = x^3 + ax + b \bmod q$, $a, b, x, y \in F_q$
pk_A	full public key of any node n_A, $pk_A = (P_A, R_A)$
sk_A	full private key of any node n_A, $sk_A = (d_A, x_A)$
K^0_A	Individual key of any node n_A
K_{AB}	Pairwise master key between n_A and n_B
k_{AB}	Pairwise encryption key between n_A and n_B
GK_j	Cluster key shared among the nodes in the j-th cluster
$\mathfrak{M}$	List of all the legitimate nodes in the network, maintained by the BS
$\mathfrak{R}$	List of revoked nodes, maintained by the BS
$HMAC(k, m)$	Message authentication code of m using key k
$E_k(m)$	A symmetric key encryption algorithm to encrypt a message m with a key k.

IV.SECURITY ANALYSIS:-

First, we briefly discuss the security of CL-HSC [13] which is utilized as a building block of CL-EKM. Later, we discuss how CL-EKM achieves our security goals. The CL-HSC [13] provides both confidentiality and enforceability for signcrypted messages based on the intractability of the EC-CDH1 Moreover, it is not possible to forge or expose the full private key of an entity based on the difficulty of EC-CDH, without the knowledge of both KGC's master private key and an entity's secret value. Here, the confidentiality is

defined as indicting wish ability against adaptive chosen cipher text and identity attacks (IND-CCA2) while enforceability is defined as existential enforceability against adaptive chosen messages and identity attacks (EUF-CMA). Further details on the CL-HSC scheme and its security proof are provided in [13].

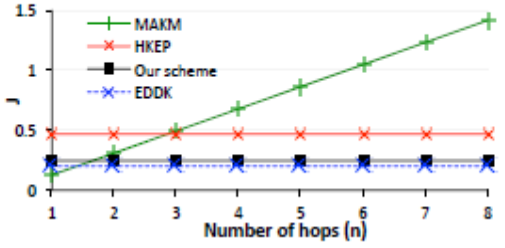
TABLE 2
Cluster Formation Process

Node Discovery and Authentication
$n_{H_j} \rightarrow *$: $\langle H_j, pk_{H_j} \rangle$
(for $i = 1, ..., n$)
$n_{L_i} \leftrightarrow n_{H_j}$: Perform *Pairwise Key Generation* phase

Cluster Key Generation
(for $i = 1, ..., n$)
n_{H_j} : Generate GK_j, Compute $C_2 = E_{k_{L_i H_j}}(GK_j, H_j, L_i)$
$n_{H_j} \rightarrow n_{L_i}$: $\langle H_j, C_2 \rangle$
n_{L_i} : Decrypt C_2 to get GK_j and
Compute $C_3 = E_{k_{L_i H_j}}(L_i, HMAC(k_{L_i H_j}, GK_j))$
$n_{L_i} \rightarrow n_{H_j}$: $\langle L_i, C_3 \rangle$
n_{H_j} : Decrypt C_3 and Check the validity

Membership Validation
n_{H_j} : Compute $C_4 = E_{K^0_{H_j}}(H_j, \mathfrak{M}_j)$, $C_5 = E_{GK_j}(H_j, \mathfrak{M}_j)$
$n_{H_j} \rightarrow$ BS : $\langle H_j, C_4 \rangle$
BS : Check $\mathfrak{M}_j$
BS $\rightarrow n_{H_j}$: $\langle Acknowledgement \rangle$
$n_{H_j} \rightarrow *$: $\langle C_5 \rangle$

Network topology



V.CONCLUSIONS AND FUTURE WORKS:-

In this paper, we propose the first certificate less effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM supports efficient communication for key updates and management when a node leaves or joins a cluster and hence ensures forward and backward key secrecy. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the information confidentiality and integrity. The experimental results demonstrate the potency of CL-EKM in resource constrained WSNs. As future work, we tend to attempt to formulate a mathematical model for energy consumption, based on CL-EKM with numerous parameters connected to node movements. This mathematical model can be utilized to estimate the correct price for the Told and Takeoff parameters supported the speed and therefore the desired trade-off between the energy consumption and the security level.

REFERENCES :

[1] W. Du, J. Deng, Y.S. Han and P. Varshney, A key predistribution scheme for sensor networks using deployment knowledge, IEEE Transactions on Dependable and Secure Computing Vol. 3, No. 1, 2006, pp. 62-77.
[2] W. Du, J. Deng, Y.S. Han, P. Varshney, J. Katz and A. Khalili, A pair wise key predistribution scheme for wireless sensor networks, ACM Trans. on Information and System Security, Vol. 8, No. 2, 2005, pp. 228-258.
[3] S. M. Rahman and K. El-Khatib, Private key agreement and secure communication for heterogeneous sensor networks, Journal of Parallel and Distributed Computing, Vol. 70, No. 8, 2010, pp. 858-870.
[4] M. R. Alagheband and M. R. Aref, Dynamic and secure key management model for hierarchical heterogeneous sensor networks,
IET Information Security, Vol. 6, No. 4, pp. 271-280, 2012.
[5] D. S. Sanchez and H. Baldus, A Deterministic Pair wise Key Predistribution Scheme for Mobile Sensor Networks, SecureComm '05.
[6] I. -H. Chuang, W. -T. Su, C. -Y. Wu, J. -P. Hsu and Y. -H. Kuo, Two-Layered Dynamic Key Management in Mobile and Long-Lived Cluster-Based Wireless Sensor Networks, IEEE WCNC 2007, pp. 4145-4150.
[7] S. Agrawal, R. Roman, M. L. Das, A. Mathuria and J. Lopez, A Novel Key Update Protocol in Mobile Sensor Networks, ICISS 2012, LNCS 7671, pp. 194-207, 2012.
[8] S. U. Khan, C. Pastrone, L. Lavagno and M. A. Spirito, An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks, CRiSIS '11, 2011.
[9] X. Zhang, J. He and Q. Wei, EDDK: Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks, EURASIP Journal on Wireless Communications and Networking, pp. 1-11, 2011.