International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5 Issue: Special 4, pp: 790-991 20 May 2016

Intelligent key administration strategies using CL-EKM over dynamic WSN

Ms. Saumya L [1]
M.Tech. Computer Science and Engineering, Cambridge Institute of Technology, K R Puram, Bangalore, India.
Ms. Jayanthi M.G [2]
Associate Professor, Dept. of CSE/ISE, Cambridge Institute of Technology, K R Puram, Bangalore, India.

***Abstract*— Now-a-days, wireless sensor networks mainly used for emerging operations such as military/army sensing units, patient monitoring system, traffic sequence analysis as well as the movement/mobility of sensor nodes from one location to another. In this case, the key requirement of the application is security, while transferring the data between source and destination. For this case apart from the normal protocol for encryption and decryption, used effective scheme like Certificate-less Effective Key Management (CL-EKM), which provides dynamically secured communication over WSNs. The CL-EKM provides energetic key changes while the node enters into the cluster region presented into the network or leave out from the network clusters. This system assists the efficient key revocation system for negotiable nodes and reduces the effect of the node adjustment for achieving security of additional security schemes. In the security investigation of this plan demonstrates that the convention is very powerful in case of safeguarding against different attacks. Here, we execute the Certificate-less Effective Key Management scheme using Windows/Linux operating system and evaluate its time, vitality and correspondence.**

***Index Terms*— Wireless Sensor Network, CL-EKM, Key Management Protocol, Key Administration Schemes**

INTRODUCTION

In today's networking environment, Dynamic Remote sensor network increase the utility of sensor nodes, boost the scope of the system, which is most effective than static wireless sensor network. In this manner, dynamic wireless sensor networks are quickly accepted by checking systems, for example, mainly used in the applications such as destination identifying in War field, medical systems and traffic monitoring systems [9]. The certificate key management schemes in past systems prove its efficiency in various terminologies, but all are often failed to work or perform only in certain limitations when the network level will go higher and the bandwidth requirement is more to attain successful ratios. So, that a new approach is required to support or solve these kinds of problems.

Along these lines, main problem facing in dynamic wireless sensor network is the security. Dynamic wireless sensor networks need to take care of additional key security preconditions, for example, node verification, message privacy and respectability, based on the node mobility.

In order to increase the security of messages, we first introduced the symmetric key encryption [1]-[3]. This sort of encryption mostly applicable for the nodes as a result of their constrained vitality and preparing ability. However, in many cases it needed vast storage space for storing pair-wise keys and also experiences more overhead. So the network lacks scalability property and also not volatile towards bargains. Because of this lack of features symmetric key encryption not acceptable for wireless sensor networks. After conducting long research, asymmetric key encryption scheduled for dynamic wireless sensor networks [4]-[7], [10], [15], [18], [21]. These different types of methodologies exploit public key cryptography (PKC), for example, elliptic curve cryptography or also the identity based public key cryptography to exchange the keys and messages among the nodes.

Generally, public key cryptography is costlier when compared with the symmetric key. Latest experiments in the elliptical curve cryptography help to increase the work-ability of public key cryptography in the WSNs [11]. Case in point, 160bit elliptic curve cryptography executed on an ATmega128 Atmel, consisting of 8-bit 8 MHz CPU, demonstrates that multiplication with elliptic curve cryptography can achieve under a second [11]. Besides, public key cryptography is stronger in node trade- off assaults and also increases versatility and adaptability. However, existing elliptic curve cryptography plans also has some security shortcomings [5], [10], [21] which includes information hacking, known key

assaults and trading off of keys. Additionally, we identified the lack security occurred due to the exposure of static private key to other node when the two nodes set up the session key. Additionally, this elliptic curve cryptography schemes are used for the sensor nodes in dynamic wireless sensor, experiences an ill effects of authentication administration overhead, which seems to be not useful for a huge scale sensor networks. The matching operation provided by the ID-PKC [4], [18] plans comes wasteful because of the computational overhead to pairing actions.

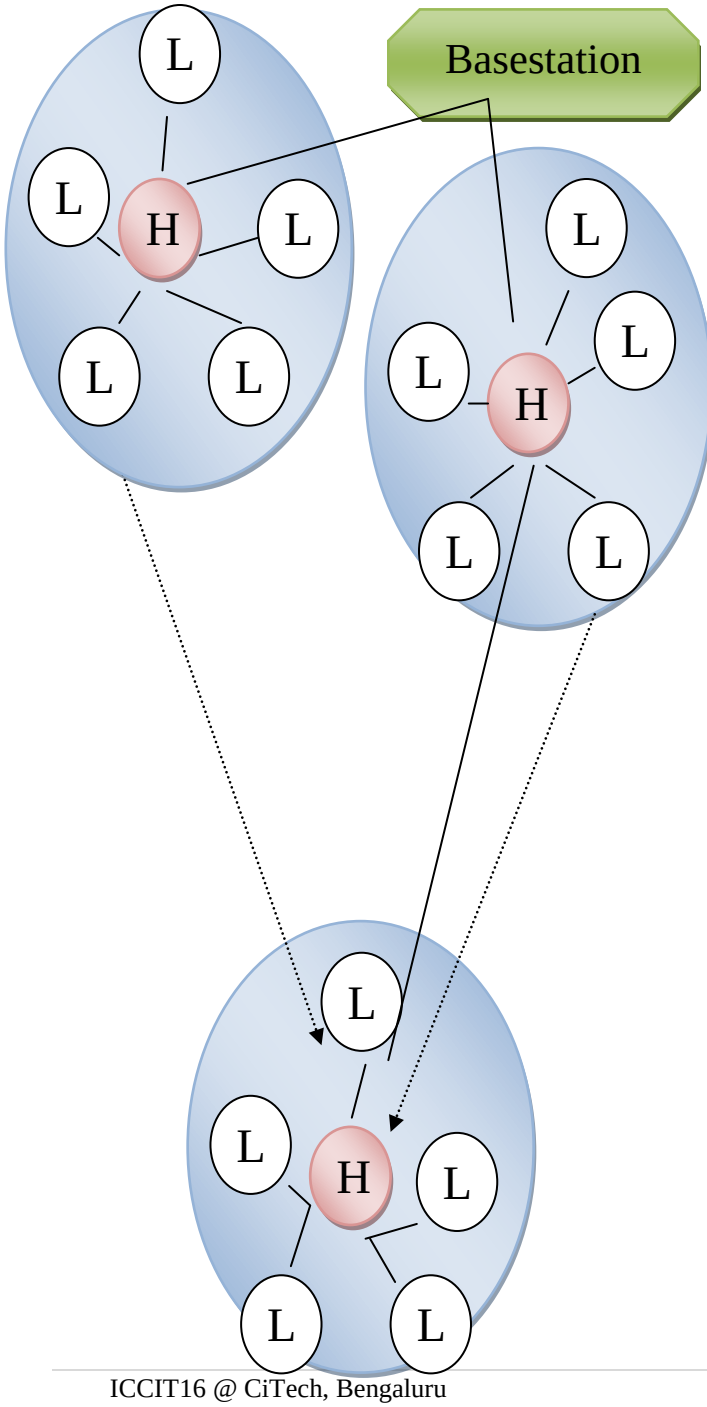


Figure.1. Wireless Sensor Network – Heterogeneous Form

Considering from all available information, we are unable to find a best, proficient and a secured key administration plans suitable for WSNs. In this paper, an effective scheme like Certificate-less Effective Key Management [CL-EKM] plan is introduced for dynamic wireless sensor networks. In case of a Certificate-less Public Key Cryptography [CL-PKC] [12], the client's full private key is consider as a blend of portion of private key created by a Key Generation Center [KGC] and the client created secret code. The exceptional association of this type of full private/public key pair evacuates the usage of Certificates also avoid the escrow issue. We additionally take the advantage of elliptic curve cryptographic keys characterized on an added substance cluster with a 160-bit length with security ensured like RSA keys having a 1024-bit length.

NODE VERIFICATION

For establishing a pairwise key between the participating sensor nodes and also to set up a node verification, we frame CL-EKM by accepting a CL-HSC that is pairing free certificate-less hybrid signcryption plan that suggested in the previous studies [13],[14]. CL-HSC helps to avert the tedious pairing key operations and also the sharing of the certificates and also allow the pair-wise key used by the CL-EKM to effectively share between the nodes. In order to bolster the node portability, the CertificateLess-Effective Key Management scheme invokes the trivial processes like the cluster key updation which occurs while the node moves and also performs a key revocation processes when the node found as the malicious node or when any node abdicate from the cluster. A CertificateLess-Effective Key Management is adaptable if there should be an occurrence of augmentations of new nodes after system establishment. A CertificateLess-Effective Key Management plan helps to attain the security from node bargain, cloning and adversary attacks [20], and also guarantees the forward and in reverse mystery. Security investigation of this plan demonstrates its viability.

CONTRIBUTIONS OF THE SYSTEM

In this paper we demonstrate some of the security shortcomings in the existing ECC plans depend on key administration plans for dynamic wireless sensor networks.

Here, we describe the main Certificateless Effective Key Management Scheme [CL-EKM] [22] for a dynamic wireless sensor networks . CL-EKM mainly includes four sorts of keys, each is utilized for an alternate reason, consisting of secure

pairwise sharing between the node and cluster key correspondence inside the groups. Effective key administration techniques are characterized as aiding node developments crosswise over various groups and key renouncement process for traded off nodes.

Certificateless effective key management scheme is actualized utilizing Windows OS and utilize a NS2 to gauge the calculation and correspondence overhead of CL-EKM [22]. Additionally, we build up a test system to gauge the vitality utilization of Certificateless Effective Key Management Scheme. At that point, we lead the reenactment of node development by embracing the Random Walk Mobility Model and the Manhattan Mobility Model inside the lattice. The trial results demonstrate that the CL-EKM plan is trivial and consequently apt for dynamic wireless sensor networks.

PAST APPROACHES AND ANALYSIS

Past analysis specified that the symmetric key encryption is only suited for static WSNs, since it cannot support the mobility of the sensor nodes. Many approaches are introduced related to Public Key Cryptography to bolster dynamic wireless sensor networks. Subsequently, we audit past PKC-depend key administration plans for the sensor nodes in WSNs and also examine the security shortcomings. Chuang et al. [7] what's more, Agrawal et al.[8] introduced an effective two-layered key administration plan and also the key updation of each sensor nodes in the WSNs. The above two plans [7],[8] are not suited for sensor nodes with restricted resources and also unable to perform costly calculations having expansive key size.

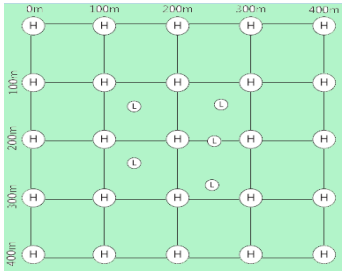


Figure.2. Network Topology Simulation

Since, Elliptic Curve Cryptography is totally very effective which requires only a precise key length [For instance, 160 bit], a few methodologies with testament [5], [10], [15] are introduced in the view of elliptic curve cryptography. However, each node requires to share the certificate to set up the pairwise key and also needed to check the certificates one another before in use, thereby increase the communication and the overhead due to calculation. Base station also suffers overhead drastically. So the already existed schemes are not sufficient for node mobility. Idea of key management using elliptic curve cryptography with signcryption suggested by Alagheband et al.[5] and Huang et al. [15] are not valid schemes since the schemes are insecure towards the adversary attacks [16].

Second of their plan, a sensor node N transmit y = qN • H(McKey) + dN (modn) to another node M for verification, where qN takes as static private key of N. In any case, once M gets the y, it can reveal qN, in light of the fact that M as of now got McKey and dN in the first step.

In this way, M can undoubtedly get qN by registering qN = (y− dN) • $H(McKey)^{-1}$. Accordingly, the private key of sensor nodes is presented to the next node while sharing the key between the two sensor nodes. A new approach that utilizes the symmetric key encryption schemes for exchanging keys only for existing sensor nodes and asymmetric encryption key scheme to exchange the pairwise key for the new sensor node is suggested by Zhang et al. [10]. Nonetheless, the starting individual key K, which is used as pairwise key after node establishment, if the foe gets K, then the foe can figure out all the individual and the pairwise key generated for all nodes. Consequently, these plans experiences frail strength to node bargains. Likewise, since such plan utilizes a basic Elliptic Curve Cryptography established Diffie Hellman key by utilizing every node's public and private key, also the common pairwise key used is static which results insecurity against known-key assaults and can't give re-key functions. Du et al.[21] utilize an Elliptic Curve Digital Signature Algorithm (ECDSA) plan to confirm the identification of cluster key head and also uses a static elliptic curve Diffie Hellman key agreement scheme.

Since, the pairwise key exchange between the cluster head is static, the Du et al [21] scheme is insecure towards the known-key assaults. Then again, Du et al. utilize a measured number juggling established symmetric key way for exchanging the pairwise key with the sensor nodes and the cluster head. So a node can't specifically set up a node pairwise key with another node since it needs the backing off from the group heads.

For this plan, if a sensor node needs to build a pairwise key with another node in the same cluster, the pairwise key is randomly generated by the cluster head and encrypts with the shared keys. After that, the cluster head sends the encrypted pairwise key to each node. However, if any of the cluster head is bargained, then the pairwise keys of the non-bargained sensor nodes present in the same cluster will likewise be traded off. Hence, their plan were not trade-off flexible against group heads attack, in light of the fact that the cluster head arbitrarily creates a pairwise key between sensor nodes at whatever point it is asked for by the nodes.

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

Also, according to their plan pairwise key sharing between two nodes in different regions should communicate with their cluster head. One cluster head will generate the pairwise key for both the nodes and send to the other cluster region and also to the its node. This pairwise key is encrypted using the shared key in both the cluster region. This scheme also supports the forward and the backward mystery [21]. However, the scheme is in secure towards clone and adversary attack.

As of late, Rahman et al. [4] what's more, Chatterjee et al. [18] suggested identity based public key cryptography that supports the portability of the node without any communication issues in the dynamic wireless sensor networks which uproots the communication overhead. Notwithstanding, their plans needed costly blending functions.

I. EXISTING METHOD ANALYSIS

In the Existing System mainly utilizes the symmetric key encryption schemes and also followed a key established methodologies are used for the dynamic wireless sensor networks. This type of deviated key based methodologies causes the security shortcomings of already existed Elliptic Curve Cryptography related plans that these methodologies are powerless against message phony, key bargain and key assaults. Since this scheme supports the static private key, node mobility has been restricted for the sensor node.

When the elliptic curve cryptography predicated schemes with certificates is precisely applied to dynamic WSNs, it experiences the certificate management overhead from all the wireless sensor nodes, which restricts the scalability of wireless sensor networks. The ID-PKC schemes which help for the pairing functions inefficient due to the computational overhead.

Disadvantages

- ✓ Vulnerably susceptible to malevolent assaults such as impersonation, interception, capture or physical eradication, because of their unattended functional environments and lacks connectivity in wireless network communication.
- ✓ One important paramount issue in many critical dynamic wireless sensor applications is the security. Symmetric key encryption causes high communication overhead and also more space needed for store the shared and pairwise keys [9]. It restricts the network scalability and the node mobility and also not strong against the compromises.
- ✓ Asymmetric encryption key also causes the certificate management overhead for all the nodes in the sensor networks. So not suitable for the large sensor networks.

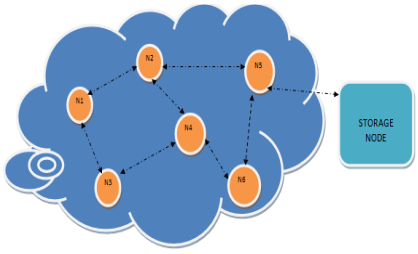
II. PROPOSED METHOD ANALYSIS

In this section, an effective scheme like CertificateLess-Effective Key Management [CL-EKM] plan is introduced for dynamic wireless sensor networks. In case of a Certificateless Public Key Cryptography [CL-PKC] [12], the client's full private key is consider as a blend of portion of private key created by a Key Generation Center [KGC] and the client created secret code. The exceptional association of this type of full private/public key pair evacuates the usage of certificates also avoid the escrow issue. We additionally take the advantage of elliptic curve cryptographic keys characterized on an added substance cluster with a 160-bit length with security ensured like RSA keys having a 1024-bit length.

Advantages

- ✓ Inorder to bolster node versatility, the Certificateless Effective Key Management scheme [22] likewise underpins lightweight procedures help cluster key get updated when the node moves from one region to another and also allow the key revocation when one node leaves from the cluster or found the node as malicious.
- ✓ Certificateless Effective Key Management [22] is versatile if there should arise an occurrence of increases of new nodes after system organization. It provides the security against the node trade-off, cloning and also guarantees forward and in reverse mystery. This security assurance of this plan demonstrates its viability.

Figure.3.
Architectural Design



In figure 3, it shows the storage nodes which form cluster region and how communication among nodes occurs.

NODE REPLICATION

In a heterogeneous dynamic WSNs (see Figure.1), the sensor network include large number of stationary or portable sensor nodes and have a base station to control the network system and information from all nodes. Wireless sensor node are of two types[19] (i) High processing capability node (H node) (ii) low processing capability node (L node). Consider M nodes in the wireless sensor network with M1 number of H node and M2 number of L node, where M=M1+M2 and also M1<<M2. Network size can change drastically because of addition and removal of nodes in the wireless sensor networks (see Figure

doi : 10.17950/ijer/v5i4/019

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

2). The H sensor node mainly considered as the cluster heads and L sensor node is considered as cluster members. These nodes are connected to the base station directly or indirectly through other H sensor node. These H and L sensor nodes can be mobile or stationary. Once a network is established every H sensor node forms a cluster with nearby L sensor node with the exchange of messages. L sensor node can combine with new cluster and also can combine with previous cluster region. The base station collects all the information from the nodes in the sensor networks and also updates the current status of all the nodes when any changes occur.

The base stations refer every node with a unique identifier. Here, L sensor node Ln is identified as IDLn and the H sensor node Hm is identified as IDHm. The base station subsist Key Generation center (KGC) which generates the four keys of Certificateless Effective Key Management scheme. The Key Generation Center mainly issues the certificate-less private key or public key, individual key, cluster key and pair-wise key.

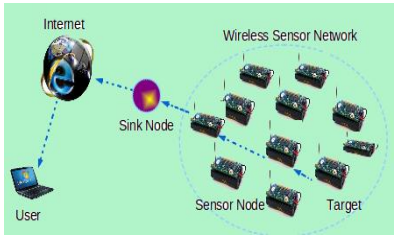


Figure.4. Wireless Network - System Model

In figure.4, it shows the information send from the user reaches the sink node via internet, the sink node send the data to the cluster region with nodes. Transmission involved security enhancing process like encryption with CL-EKM [22] scheme. Data transmitted from one node to the other utilizing the CL-EKM [22] scheme reaches the destination node.

LITERATURE SURVEY

In [1][2] "New adversary and new threats: Security in unattended sensor networks", the authors D. Ma, C. Soriente, quoted on, this system is to easy to find out the Unattended nodes but the major disadvantage of this system is it takes more time to process the node attributes.

In [3] "SCARKER: A sensor capture resistance and key refreshing scheme for mobile WSNs", the authors Y. Ren, V. Oleshchuk, F. Y. Li, quoted on, this system sensor Capture Resistance values are so high, so that the performance is good, however it is very hard to achieve the standards of data transmissions.

In [4] "Catch me (if you can): Data survival in unattended sensor networks", the authors R. Di Pietro, L. V. Mancini, quoted on, this system is contains an efficient Data Survival Mechanisms are implemented but causes failure in case of large set of data transmissions.

In [5] "United we stand: Intrusion-resilience in mobile unattended WSNs", the authors R. Di Pietro, G. Oligeri, C. Soriente, quoted on, Implementing encroachment free network architecture, but it causes Many confusions while if the nodes range is large or long transmissions.

In [6] "A trust-based geographical routing scheme in sensor networks", the authors K.-S. Hung, K. S. Lui, and Y.K. Kwok, quoted on, in this system the trust Based Data transmission Scheme are used, but it requires more and more complicated functions to handle with for manipulating trust over nodes.

In [7] "TARP: A trust-aware routing protocol for sensor-actuator networks", the authors A. Rezgui and M. Eltoweissy, quoted on, in this system trustworthy Routing environments are formed and the implementation of Probabilistic approach is fully followed.

CERTIFICATE-LESS EFFECTIVE KEY MANAGEMENT

Certitificate-less Effective Key Management scheme mainly works based on four keys namely: certificate-less public/private Key, pairwise key, individual key and cluster Key. These schemes utilize the concept of CL-HSC scheme. The keys are mainly generated by the Key Generation Center (KGC) in base station. Generated keys can be explained as:

- *Certificateless Public/Private Key :* This key pair is generated by the Key Generation Center (KGC) before the node deployment. It installs the keys in the generated node. Pairwise key is generated from this key pair.
- *Individual Key:* Every node exchanges a unique individual key with the base station. This key is used for encrypting the alert message send to the base station. Base station also uses the individual key for encrypting the compromised node information.
- *Pairwise Key:* Every node exchanges a distinct pairwise key for the communication with the nearby nodes. In the wireless sensor network the L sensor node utilizes the pairwise key to transmit the data securely to the nearby H sensor node.
- *Cluster Key:* Every node in the cluster is identified using the cluster key. This key is used to transmit the data within the cluster and also with another cluster. It requires only the change in the cluster head, in case of any updation in the sensor node.

doi : 10.17950/ijer/v5i4/019

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

EXPERIMENTAL RESULTS

Figure.5. Input Parameters

In figure. 5, indicates the input parameters, based on this input, nodes are created and form three cluster regions. Considering the input parameters like average network traffic flow, traffic strength, packet transmission speed and packet dropping rate, the information transmitted between the nodes using the encoding and encryption with CL-EKM scheme. Detailed view of the transmission shown below. Here, CL-EKM scheme helps the node mobility from one region to the other and destination node can also have the node mobility from one region to the other. Encryption of encoded data enhances the security for data.

Figure.6. Encoded Data

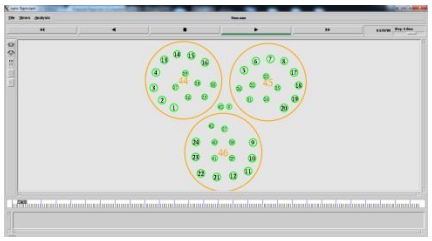


Figure.7. Wireless Nodes Creation

Figure.8. Nodes Communication in WSN

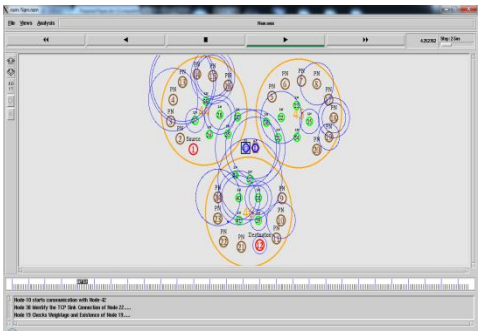


Figure.9. Node Mobility across Wireless Regions

Figure.10. Node Mobility to Next Region

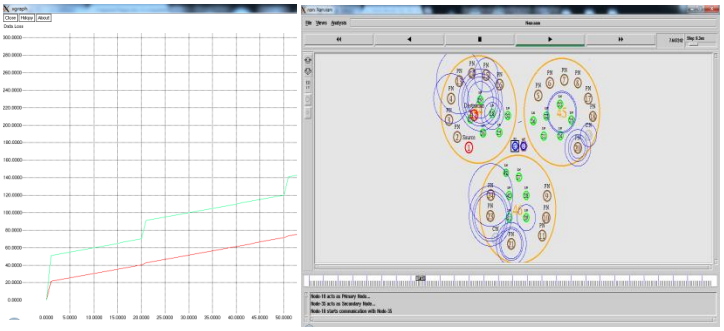


Figure.11. Data Loss Analysis

Source Node	Dest. Node	Average N/w Traffic	Traffic Strength	Packet Trans-mission Speed	Packet Dropping Rate
1	12	26	130	35	15

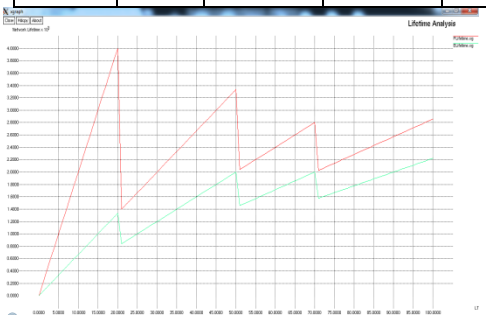


Figure.12. Lifetime Analysis

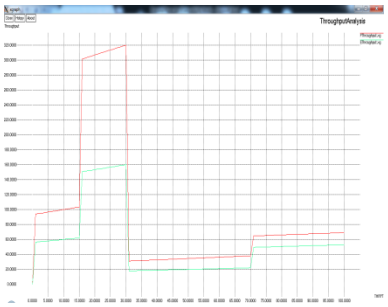


Figure.13. Throughput Analysis

doi : 10.17950/ijer/v5i4/019

ISSN:2319-6890)(online),2347-5013(print)
20 May 2016

Figure.14. Energy Consumption Analysis

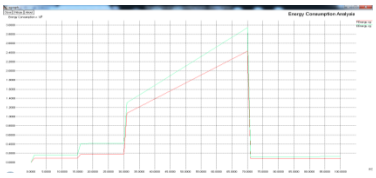


Figure. 11-14 shows the graphical analysis based on the given input parameters. Here, we generate the data loss analysis, lifetime analysis, throughput analysis and energy consumption analysis. Data loss and energy consumption of the proposed system are less when compared to the existing system. Lifetime and throughput are more in proposed than the existing. Here, in the data loss analysis graph (see Figure.11), data loss is mainly, based on the input parameter packet dropping rate. When the packet dropping rate increases the data loss will also increases.

In the Lifetime Analysis graph (see Figure.12) the lifetime depends on the average network traffic flow. When the traffic increases the lifetime also increases. In the throughput analysis (see Figure.13), through put depends on the input parameters packet transmission speed, when the transmission speed increases the through put also get increases. In the Energy consumption analysis (see Figure.14), energy consumption depends on individual traffic strength when the traffic strength increases the energy consumption also will increases.

CONCLUSION

Certificate-less Effective Key Management scheme helps for the secure message exchange between the sensor nodes in the dynamic wireless sensor networks. This scheme helps the proper key updation and the administration for addition and removal of sensor nodes in the WSNs. It also provides the forward and the backward mystery. This scheme provides security towards compromise node, adversary attack, impersonation, cloning and also provide data integrity and confidentiality. The output from the experiments indicates the effectiveness of the scheme when used in the wireless sensor networks. In future, we can add a mathematical design for energy consumption that works with different parameters based on the node movement.

REFERENCES

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

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

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

[4] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," J. Parallel Distrib. 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. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012.

[6] D. S. Sanchez and H. Baldus, "A deterministic pairwise key predistribution scheme for mobile sensor networks," in Proc. 1st Int. Conf. SecureComm, Sep. 2005, pp. 277–288.

[7] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Twolayered dynamic key management in mobile and long-lived cluster based wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.

[8] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in Proc. 8th Int. Conf. ICISS, vol. 7671. 2012, pp. 194–207.

[9] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, "An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks," in Proc. 6th Int. Conf. CRiSIS, Sep. 2011, pp. 1–8.

[10] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," EURASIP J. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.

[11] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst., 2004, pp. 119–132.