International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

CL-EKM Protocol for Secure Communication in Dynamic Wireless Sensor Networks

[1]**Rapolu Praveen Kumar** M. Tech. (PhD) – Assistant Professor (praveenkumarrapolu@gmail.com)

[2]**Greeshmasai** (greeshmasai2014@gmail.com)

[3]**SanjayKumar** (sanjaysanjugoud.s@gmail.com)

[4]**Taruni** (tarunireddy88@gmail.com)

[1, 2, 3,4]Dept.of Computer Science and Engineering, Vignan Institute of Technology and Science, Deshmukhi, Hyderabad. 508284

Abstract:

Recently, wireless sensor networks (WSNs) have been deployed for a wide variety of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring, where sensory devices often move between different locations. Securing data and communications requires suitable encryption key protocols. In this paper, we propose a certificate less-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks. We implement CL-EKM scheme and simulate it using a simulator to assess its time, energy, communication, and memory performance.

In this paper, we present a CL-EKM scheme for dynamic WSNs. In 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..

Keywords

CL-EKM: Certificate Less Effective Key Management.CL-PKC: Certificate Less Public Key Cryptography.CL-HSC: certificate less hybrid signal encryption scheme...

1. Introduction

A. Motivation

Dynamic wireless sensor networks (WSNs), which enable mobility of sensor nodes, facilitate wider network coverage and more accurate service than static WSNs. Therefore, dynamic WSNs are being rapidly adopted in monitoring applications, such as target tracking in battlefield surveillance, healthcare systems, traffic flow and vehicle status monitoring, dairy cattle health monitoring. However, sensor devices are vulnerable to malicious attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of connectivity in wireless communication. Thus, security is one of the most important issues in many critical dynamic WSN applications.

Dynamic WSNs thus need to address key security requirements, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move. To address security, encryption key management protocols for dynamic WSNs have been proposed in the past based on symmetric key encryption. Such type of encryption is well-suited for sensor nodes because of their limited energy and processing capability. However, it suffers from high communication overhead and requires large memory space to store shared pair wise keys. It is also not scalable and not resilient against compromises, and unable to support node mobility.

Therefore symmetric key encryption is not suitable for dynamic WSNs. More recently, asymmetric key based approaches have been proposed for dynamic WSNs.

B. Objective

In this paper, we present a certificate less effective key management (CL-EKM) scheme for dynamic WSNs. In certificate less 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[1][2][3] 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 signecryption scheme (CL-HSC) proposed by us in an earlier work, Due to the properties of CL-HSC, the pairwise key of CL-EKM can be efficiently shared between two nodes without requiring taxing pairing operations and the exchange of certificates. 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. Below we summarize the contributions of this paper:

• We show the security weaknesses of existing ECC based key management schemes for dynamic WSNs.

• We propose the first certificateless 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.

• CL-EKM is implemented using Contiki OS and use a TI exp5438 emulator to measure the computation and communication overhead of CL-EKM. 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.

The experimental results show that our CL-EKM scheme is lightweight and hence suitable for dynamic WSNs.

C. Types of Keys:

• Certificateless Public/Private Key: Before a node is deployed, the KGC at the BS generates a unique certificateless private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pairwise key[3].

• Individual Node Key: Each node shares a unique individual key with BS. For example, a L-sensor can use the individual key to encrypt an alert message sent to the BS, or if it fails to communicate with the H-sensor. An H-sensor can use its individual key to encrypt the message corresponding to changes in the cluster. The BS can also use this key to encrypt any sensitive data, such as compromised node information or commands. Before a node is deployed, the BS assigns the node the individual key.

• Pairwise Key: Each node shares a different pairwise key with each of its neighboring nodes for secure communications and authentication of these nodes. For example, in order to join a cluster, a L-sensor should share a pairwise key with the H-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by using the pairwise key. In an aggregation supportive WSN, the L-sensor can use its pairwise key to securely transmit the sensed data to the H-sensor. Each node can dynamically establish the pairwise key between itself and another node using their respective certificateless public/private key pairs[25][26].

• Cluster Key: All nodes in a cluster share a key, named as cluster key. The cluster key is mainly used for securing broadcast messages in a cluster, e.g., sensitive commands or the change of member status in a cluster. Only the cluster head can update the cluster key when a L-sensor leaves or joins the cluster.

D. RELATED WORK:

Symmetric key schemes are not viable for mobile sensor nodes and thus past approaches have focused only on static WSNs. A few approaches have been proposed based on PKC to support dynamic WSNs. Thus, in this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al.and Agrawal et al. proposed a two-layered key management scheme and a dynamic key update protocol in dynamic WSNs based on the Diffie-Hellman (DH), respectively. However, both schemes are not suited for sensors with limited resources and are unable to perform expensive computations with large key sizes (e.g. at least 1024 bit). Since ECC is computationally more efficient and has a short key length (e.g. 160 bit), several approaches with certificate have been proposed based on ECC[11][12][13]. However, since each node must exchange the certificate to establish the pairwise key and verify each other's certificate before use, the communication and computation overhead increase dramatically.

2. Literature review

a. *Compressive Sensing Over Networks:*

In this system, we demonstrate some applications of compressive sensing over networks.

We make a connection between compressive sensing and traditional information theoretic techniques in source coding and channel coding. Our results provide an explicit trade-off between the rate and the decoding complexity. The key difference of compressive sensing and traditional information theoretic approaches is at their decoding side. Although optimal decoders to recover the original signal, compressed by source coding have high complexity, the compressive sensing decoder is a linear or convex optimization. First, we investigate applications of compressive sensing on distributed compression of correlated sources. Here, by using compressive sensing, we propose a compression scheme for a family of correlated sources with a modularized decoder, providing a trade-off between the compression rate and the decoding complexity.

We call this scheme Sparse Distributed Compression [21][22]. We use this compression scheme for a general multicast network with correlated sources. Here, we first decode some of the sources by a network decoding technique and then, we use a compressive sensing decoder to obtain the whole sources. Then, we investigate applications of compressive sensing on channel coding. We propose a coding scheme that combines compressive sensing and random channel coding for a high-SNR point-to-point Gaussian channel. We call this scheme Sparse Channel Coding. We propose a modularized decoder providing a trade-off between the capacity loss and the decoding complexity. At the receiver side, first, we use a compressive sensing decoder on a noisy signal to obtain a noisy estimate of the original signal and then, we apply a traditional channel coding decoder to find the original signal.

b. *Compressive Data Gathering for Large-Scale Wireless Sensor Networks*

This system presents the first complete design to apply compressive sampling theory to sensor data gathering for large scale wireless sensor networks. The successful scheme developed in this research is expected to offer fresh frame of mind for research in both compressive sampling applications and large-scale wireless sensor networks. We consider the scenario in which a large number of sensor nodes are densely deployed and sensor readings are spatially correlated. The proposed compressive data gathering is able to reduce global scale communication cost without introducing intensive computation or complicated transmission control. The load balancing characteristic is capable of extending the lifetime of the entire sensor network as well as individual sensors. Furthermore, the proposed scheme can cope with abnormal sensor readings gracefully. We also carry out the analysis of the network capacity of the proposed compressive data gathering and validate the analysis through ns-2 simulations.

More importantly, this novel compressive data gathering has been tested on real sensor data and the results show the efficiency and robustness of the proposed scheme.

c. *Compressive Data Gathering Scheme for Wireless Sensor network-a review*

In this system, we present a brief review of compressive sensing (CS) applied to the wireless sensor web. In wireless sensor networks (WSNs) the sampling rate of the sensors determines the pace of its energy use since most of the energy is used in sampling and transmission. To economize the energy in WSNs and thus extend the network lifetime, CS theory used to downplay the number of samples taken by sensor nodes. And also CS finds its applications in information gathering for large wireless sensor networks (WSNs)[21] , consisting of thousands of sensors deployed for tasks like infrastructure or environmental monitoring. This advance of using compressive data gathering (CDG) helps in overcoming the challenges of high communication costs.

d. *Random Access Compressed Sensing in Underwater Sensor Networks*

In this system, we propose a power-efficient underwater sensor network scheme employing compressed sensing and random channel access. The proposed scheme is suitable for applications where a large number of sensor nodes are deployed uniformly over a certain area to measure a physical phenomenon. The underlying assumption is that most physical phenomena have sparse representations in the frequency domain. The network is assumed to have a Fusion Center (FC) that collects the observations of sensor nodes and reconstructs the measured field based on the obtained measurements.

The proposed method is completely decentralized, i.e., sensor nodes act independently without the need for coordination with each other or with the FC. During each frame, a Bernoulli random generator at each node determines whether the node participates in sampling or stays inactive during that sampling period. If selected, it measures the physical quantity of interest, e.g. temperature. A second random generator with a uniform distribution then picks a (random) delay for the node to send its data to the FC. The proposed network scheme, referred to as Random Access Compressed Sensing (RACS), results in a simple power-efficient design, for: a) it

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

eliminates the need for duplexing, which requires coordination from the FC; b) there is no need for acknowledgment packets and retransmissions in case packets collide; and moreover, c) it is efficient in terms of the communication resources used (only a small fraction of nodes sample and transmit in each sampling period).

e. Signal Recovery from Random Measurements via Orthogonal Matching Pursuit

This system demonstrates theoretically and empirically that a greedy algorithm called Orthogonal Matching Pursuit (OMP) can reliably recover a signal with m nonzero entries in dimension d given O (mln d) random linear measurements of that signal. This is a massive improvement over previous results, which require O (m2) measurements. The new results for OMP are comparable with recent results for another approach called Basis Pursuit (BP). In some settings, the OMP algorithm is faster and easier to implement, so it is an attractive alternative to BP for signal recovery problems.

3. System Design and Architecture

The system architecture explain the functioning of modules and accessing the transfer of secure data from client and server through cluster, nodes and sensors:

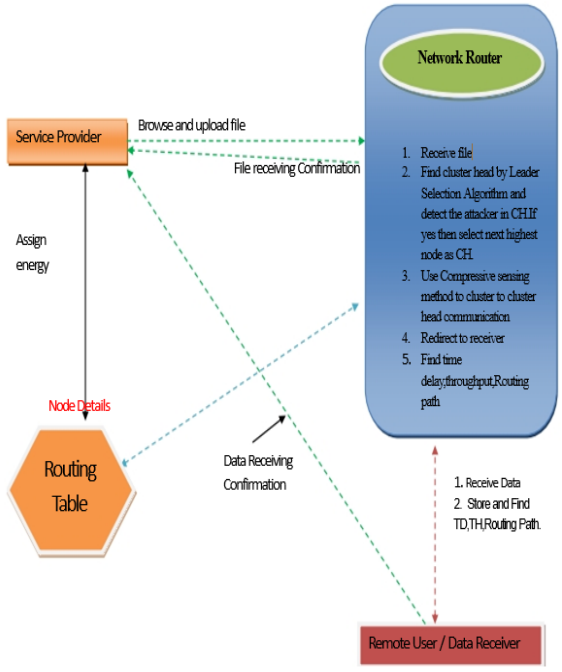

Fig 1: Architecture diagram

SDLC (Umbrella Model):

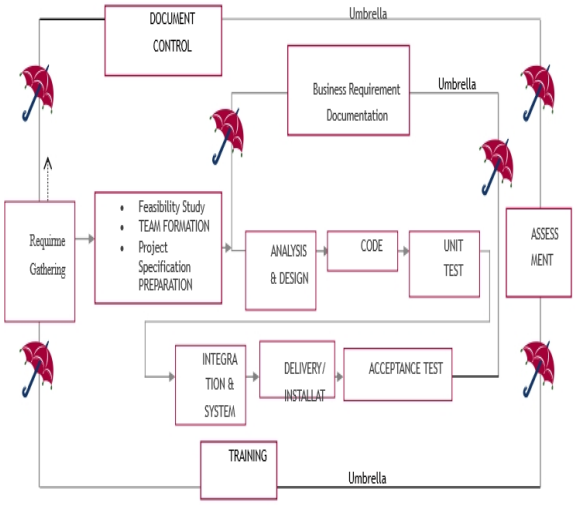

Fig 2: SDLC phases.

SDLC is nothing but Software Development Life Cycle. It is a standard which is used by software industry to develop good software.

Stages in SDLC:

- Requirement Gathering
- Analysis
- Designing
- Coding
- Testing
- Maintenance

A. Input Design:

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms

have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

B. Output Design

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him.

After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only.

The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

C. 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 unforgeability for signcrypted messages based on the intractability of theEC-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 andan entity's secret value. Here, the confidentiality is defined as indistinguishability against adaptive chosen cipher text and identity attacks (IND-CCA2) while unforgeability is defined as existential unforgeability against adaptive chosen messages and identity attacks (EUF- CMA). Further details on the CL-HSC scheme and its security proof are provided in [13].

D. Existing System:

• Existing System make use of different techniques like symmetric key encryption and asymmetric key based approaches for developing dynamic WSNs.

•Asymmetric key based approaches proved that the security weaknesses of existing ECC (Elliptic curve cryptography)-based approaches are vulnerable to message forgery, key compromise and addition of duplicate data. Also, we analyzed the critical security flaws of the static private key is exposed to the others when both nodes establish the session key.

•Moreover, if these ECC-based schemes with certificates are directly applied on dynamic WSNs, they suffer from the certificate management overhead between all sensor nodes which are not applicable in large scale WSNs.

Drawbacks Of Existing System:

•Existing Sensor devices are vulnerable to malicious attacks such as intruders, interception, capture or physical destruction, due to their errors in establishing connectivity in wireless communication.

•Asymmetric key based approaches suffer from the certificate management overhead of the entire sensor nodes and so are not a practical application for large scale WSNs.

•Symmetric key encryption suffers from high communication overhead and requires large memory space to store shared pair wise keys. It is also not scalable and unable to support node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs.

E. Proposed System:

•In this paper, we present a CL-EKM scheme for dynamic WSNs. Here we make use of "certificate less public key cryptography"(CL-PKC), where the user's full private key is used which is a combination of a partial private key 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 generation problem by removing the user's full private key.

•In order to provide node authentication and pair wise key between nodes, we build CL-EKM by utilizing a pairing-free certificate less hybrid signal encryption scheme (CL-HSES).

Advantages Of Proposed System:

•To support node accessing, CL-EKM make use of light weight processes to notify the cluster key updates when a node moves.

•CL-EKM is scalable in case of additions of new nodes.

•CL-EKM is secure against node compromise and ensures forward and backward secrecy. The security analysis of our scheme shows its effectiveness.

F. Modules implementation:

We make use of five type of modules to implement the exceution of CLEKM protocol they are:

1. Service provider:

In this module, the service provider will browse the data file and then send to the particular receivers. Service provider will send their data file to router and router will connect to clusters, in a cluster highest energy sensor node will be activated and send to particular receiver (A, B, C…). And if any attacker will change the energy of the particular sensor node, then service provider will reassign the energy for sensor node.

2. Router:

The Router manages a multiple clusters (cluster1, cluster2, cluster3, and cluster4) to provide data storage service. In cluster n-number of nodes (n1, n2, n3, n4…) are present, and in a cluster the sensor node which have more energy considered as a cluster head and it will communicate first. In a router service provider can view the node details, view routing path, view time delay and view attackers. Router will accept the file from the service provider, the cluster head will select first and it size will reduced according to the file size, then next time when we send the file, the other node will be cluster head. Similarly, the cluster head will select different node based on highest energy. The time delay will be calculated based on the routing delay.

3. Cluster:

In cluster n-number nodes are present and the clusters are communicates with every clusters (cluster1, cluster2, cluster3 and cluster4).In a cluster the sensor node which have more energy considered as a cluster head. The service provider will assign the energy for each & every node. The service provider will upload the data file to the router; in a router clusters are activated and the cluster-based networks, to select the highest energy sensor nodes, and send to particular receivers.

4. Receiver (End User):

In this module, the receiver can receive the data file from the service provider via router.

The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

5. Attacker:

Attacker is one who is injecting the fake energy to the corresponding sensor nodes. The attacker decries the energy to the particular sensor node. After attacking the nodes, energy will be changed in a router.

4. Results

Fig 3: Browsing file

This figure is the initial screen which would explain the information about browsing the file and setting the path. The procedure to execute is

1. Click on file and select Effective key management folder.
2. Click on src folder and select data owner.java file.
3. Click on encrypt and select the mac address and click on submit.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Fig.4 Encryption process

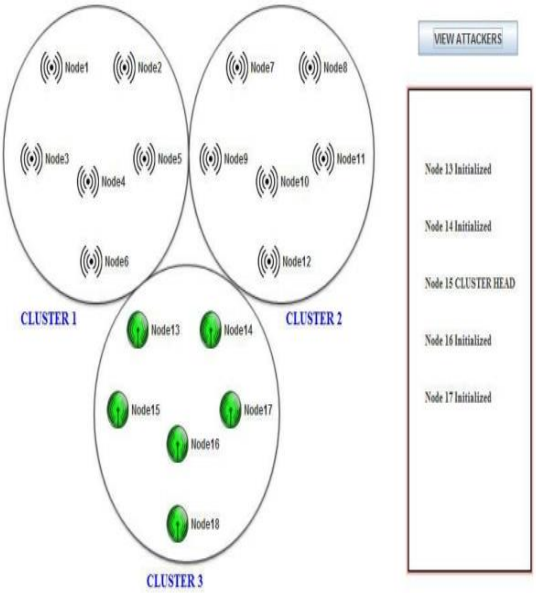

Fig.5 Node Initialization

This figure display information about the cluster and node initialization. After submitting the ip address and destination node, any of the selected cluster head would get activated and the nodes would get initialized with sensors. Nodes will be initialized based on their energy assigned.

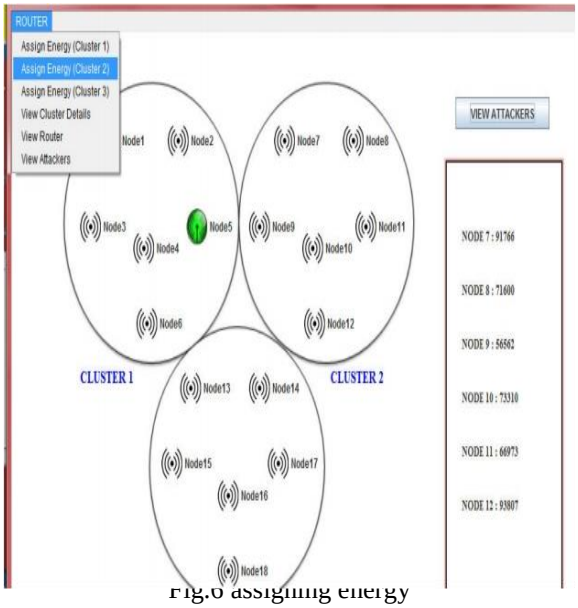

Fig.6 assigning energy

This figure explain the information about the energy assigning process of nodes and clusters. The main reason of assigning more energy is to avoid the nodes and cluster from hacking. Until all nodes are assigned with correct energy and data the encryption and sending of file process to the destination would not be started.

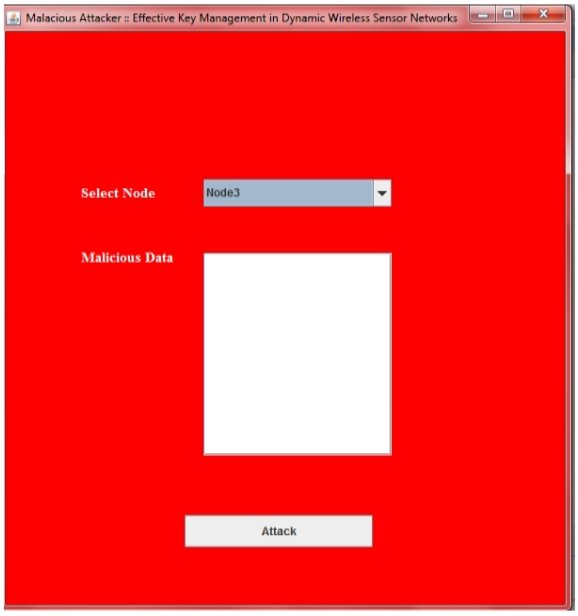

Fig.7 Malicious Attacker

This figure explain the information about process of adding the malicious data to the node to hack the cluster and the data transferring in the nodes. Here the hacker would add the malicious data into original file which has been sent. But through sensors and nodes the sending of data would be stopped until the

malicious threat and data would be captured. In this process the nodes and clusters will not be initialized. Once all the malicious data is been cleaned the original encrypted file will be stored in node head.

5. Conclusion

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 and encrypted data storage. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. The experimental results demonstrate the efficiency of CL-EKM in resource constrained WSNs. As we make use of 2 types of implementation algorithms MRSA and MD5 we can transfer the data from source to destination with efficient speed and security.

Future Enhancement:

As future work, we plan to formulate a mathematical model for energy consumption, based on CL-EKM with various parameters related to node movements. This mathematical models along with the implementation algorithms may be applicable in various large wire less sensor networks.

6. 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. Comput., 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. Secure Comm, Sep. 2005, pp. 277–288.

[7] 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," 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.

[12] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. 9th Int. Conf. ASIACRYPT, vol. 2894. 2013, pp. 452–473.

[13] S. Seo and E. Bertino, "Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing," CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR 2013-10, 2013. [Online]. Available: https://www.cerias.purdue.edu/apps/reports_and_papers/.Seung-Hyun.

[14] S. H. Seo, J. Won, and E. Bertino, "POSTER: A pairing-free certificateless hybrid sign cryption scheme for advanced metering infrastructures," in Proc. 4th ACM CODASPY, 2014, pp. 143–146.

[15] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in Proc. 2nd ACM Int. Conf. WSNA, 2003, pp. 141–150.

[16] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in Proc. IACR Cryptol. ePrint Archive, 2013, pp. 698–698.

[17] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab,"NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in Proc. 5th Eur. Conf. WSN, vol. 4913. 2016, pp. 305–320.

[18] K. Chatterjee, A. De, and D. Gupta, "An improved ID-based keymanagement scheme in wireless sensor network," in Proc. 3rd Int. Conf.ICSI, vol. 7332. 2012, pp. 351–359.

[19] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replicationattacks in mobile sensor networks: Theory and approaches," Secur.Commun. Netw., vol. 5, no. 5, pp. 496–507, 2016.

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

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

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

[23] (2013). All About Battery. [Online]. Available:http://www.allaboutbatteries.com/Energy-tables.html, accessed Dec. 2014.

[24] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proc. Int. Conf. IPSN,Apr. 2008, pp. 245–256.

[25] D. Du, H. Xiong, and H. Wang, "An efficient key management schemefor wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2012,Sep. 2012, Art. ID 406254.

[26] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 36,no. 2, pp. 611–622, 2013.

[27]URL: http://www.onjava.com
Rss: http://www.oreillynet.com/pub/feed/7?format=rss2

[28]URL: http://java.sun.com

Rss : http://developers.sun.com/rss/java.xml

[29]URL: http://www.developer.com/java/

[30]Rss: http://www.developer.com/icom_includes/feeds/developer/dev-25.xml

[31]URL: http://www.javaworld.com

Rss : http://www.javaworld.com/rss/index.html

[32]URL: http://downloadllnw.oracle.com/docs/cd/E17409_01/javase/tutorial/