Efficient Clustering and Key Management with Secure Routing in Wireless Sensor Network

Prof. Sujata Wakchaure
Assistant Professor,MAEER'S MITCOE, Kothrud Pune

Abstract-*Today wireless sensor networks are used in various applications like battlefield surveillance and dynamic wireless Sensor Network (DWSN) attained much popularity due its vast coverage and capabilities Dynamic Wireless sensor Network (DWSN) supports mobility of sensor nodes such that nodes with identical characteristics dynamically form a group which is known as a cluster. Every cluster contains a Cluster head which gather and send the aggregated data to a base station (BS). BS manages node mobility as well as authentication for each node. Hence for such systems security is a concern and there is a need of protected and energy efficient communication algorithm for these low power devices. One solution to address these security concerns for such systems is encryption key management. As of now many solutions have been put forward that use public and private key cryptographic techniques out of which ECC which is a public key cryptographic method is an efficient solution for WSN. Seung-Hyun Seo et al., introduced CL-EKM to conquer various drawbacks in existing solutions by providing low overhead for certificate exchange and more security management by using various keys like pair wise key, individual key etc. In this paper we tend to improve the security by adding redundant BS, and use HEED clustering algorithm for enhancing the energy efficiency.*

Keywords- Wireless Sensor Networks, Certificateless Public Key Cryptography, Cluster Head, Base Station, Key Management Scheme.

I. INTRODUCTION

Wireless sensor network (WSN), consist of a scads of low-cost, low-power and small sensor nodes which forms clusters. Due to its furtherance in sensing and security Dynamic WSN are in great use in innumerable applications, for example, it includes target tracking and battlefield surveillance in military, traffic flow monitoring, health care system and many more. The main task of dynamic WSNs is monitoring the target area and sends collected data from mobile sensor nodes in the target area to the Base Station (BS) using wireless channel. With increase in use there comes the increase in attacks and breaches, hence there is a need for better security solutions. In recent research EKM has proved beneficial for WSN.

Ample of asymmetric and symmetric encryption techniques for instance ECC, Attribute based encryption and Identity based encryption have been proposed to increase the security level for WSNs. As the application security mechanism depends on available strong and efficient key distribution techniques. To access the information, node should be authorized and should know the key to encrypt the data, this key and information must be inaccessible to the compromised nodes. These keys should be updated to maintain security and resilience from attacks.

Dynamic WSNs gives priority to key security concerns, such as authentication of node, key duplication, denial of service and other attacks. To conquer this, encryption and decryption using single key in symmetric key management protocol is insufficient in dynamic WSNs because of limited energy and processing capability of nodes. It faces high correspondence overhead and requires extensive memory space to store shared pairwise keys. It is prone to compromises, and unable to support node mobility. Hence, this shows that symmetric key encryption is not suitable for dynamic WSNs.

On the other hand asymmetric key based methodologies take benefits of public key cryptography (PKC) as elliptic curve cryptography (ECC) or identity-based public key cryptography (ID-PKC) so as to simplify key establishment and data validation between nodes. Symmetric key encryption is moderately cheaper than PKC with respect to computational expenses. In addition, PKC is resistant to node attacks and is more versatile and adaptable. On the other hand, ECC is powerless against message forgery, key compromise and known-key attacks. Moreover, when ECC based schemes involve certificates in dynamic WSNs, suffers from a disadvantage of certificate management overhead of all sensor nodes. There is computational overhead, because of pairing operations. Similarly ID-PKC schemes suffer from overhead due to pairing operations.

Certificateless Key management scheme [6] for WSNs consist of pairwise, individual, cluster and a groupwise key which are issued to each node through broadcast during the network composition phase and no further message exchange is required afterwards. Cluster head is

communicated by the nodes for establishing group key and pair wise key.

At last effective key management (CL-EKM) scheme without certificate for dynamic networks implements private key as a combination of a partial private key and the own secret value of users. This partial private is generated by key generation center. The procedure helps in dynamically provide both node authentication and establish pairwise key between nodes. The pairwise key of CL-EKM can be efficiently shared between two nodes. CL-EKM also supports lightweight processes for cluster key updates which is executed when a node moves, and key disapproval is executed when a node is identified as malicious or leaves the cluster permanently. CL-EKM is efficient and versatile in adding a new node after network deployment. CL-EKM provides security against compromise nodes and ensures forward and backward privacy. The security analysis of our plan demonstrates its effectiveness.

Beneath we summarize the commitments of this paper:

- We show the security weaknesses of existing system when attack is performed on cluster head.
- We propose the secure data sending to base station at the time of attack detection on cluster head in dynamic WSNs.
- We propose to elect the cluster head using Heed protocol to increase energy efficiency and to enhance the network life time in heterogeneous network.

In this paper further we will see: Section II talks about related work studied till now on topic. Section III current implementation details, introductory definitions and documentations and in addition formally expresses the proposed work undertakings tended to by this paper.

II. LITERATURE REVIEW

H. Chan e al [1], Key Generation in wireless sensor networks is complicated issue on the asymmetric key cryptosystems are inappropriate for use in source restricted sensor nodes, furthermore since the nodes could be actually affected by an attacker. They introduce three new systems for key generation using the structure of pre-distributing a unique set of secrets of each node. First, in the q-composite important factors plan, they trade off the unlike liness of a large-scale system attack to be able to considerably enhance unique key predistribution's durability against smaller-scale attacks. Second, in the multipath-reinforcement plan, they display how to enhance the protection between any two nodes by utilizing the protection of other links. Lastly, they exists the random pair wise important factors plan, which completely maintains the secrecy of the remaining system when any node is taken, and also allows node-to-node verification and majority based renouncement. Solving the security problem in resource constrained sensors network.

M. R. Alagheband et al [2] says that earlier most of the researches assign keys considering homogeneous network architecture. Later, a couple of key management models for heterogeneous WSNs were proposed with the study giving rise to dynamic key management system with the base of elliptical curve cryptography and sign encryption method for heterogeneous WSNs. Such network were improved with network scalability and sensor node (SN) mobility. additionally, both periodic verification as well as a new subscription mechanism were proposed with SN compromise. The authors analyses states that their framework independently proves to be better in terms of conversation, calculations and key storage area.

A. Wander et al. [3], put forward an algorithm to reduce the number of memory accesses in order to enhance multiple-perfection multiplication based on three observations: 1. Feasibility of Public-key cryptography on small devices. 2. ECC point multiplication proves to be better over RSA modular exponentiation rises as the processor word size decreases and the key size increases. 3. Elliptic curves over fields provide increased efficiency.

H. Kobayashi et al. [4], have proposed a hybrid authenticated key establishment system, which uses the difference in capacities between security administrators and sensors, and put the cryptographic pressure at places where sources are less restricted by taking into consideration efficient authenticated key establishment protocols in a self-organizing sensor network. Such system reduces the high cost asymmetric-key operations at the sensor side and replaces them with efficient symmetric-key based operations. Meanwhile, the scheme authenticates the two identities based on public key certificates to prevent the typical key management issue in pure symmetric-key based protocols giving better efficiency.

III. PROPOSED SYSTEM

This section discuss proposed system, system overview proposed algorithm, mathematical model of the proposed system in detail.

A. System Overview

The architectural view of the proposed system is presented in figure 1.Later work flow of the system is divided and described into various steps:

Network Generation

Initially network is generated having distributed nodes which is then analyzed, then system processing leads in development of system parameters from which some are stored at the BS and some are deployed on nodes.

Clustering Process

In this stage distributed nodes are grouped into groups or clusters based on clustering algorithm. Multiple clusters are generated in the network based on different characteristics.

Cluster Head Selection

Cluster heads for each cluster is elected HEED protocol which takes into account residual energy and communication cost of each node.

Individual Key distribution

Base station generates the key and distributes the keys to each node. Each node shares the unique individual key to the base station.

Pairwise Key distribution

This stage contributes in generating set of Pairwise Key which include Master key and Encryption key, these keys are shared between nodes.

Cluster Key distribution

Cluster head generates the cluster key at the time of cluster formation and distributes that key to each node. Each node shares the key in a cluster to for broadcasting massages.

Data Collection

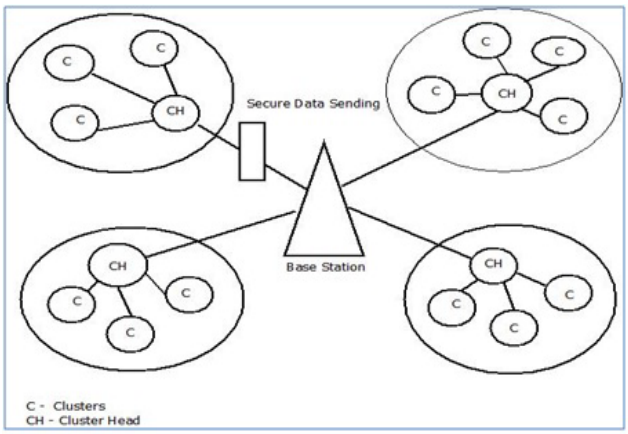

Fig 1. System Architecture

After distribution of all keys, When the system initiate nodes sense data , forward it to next node so that it reach the cluster head Cluster head collect all the data and verify it.

Data aggregation

This task of aggregation is headed by the cluster head after processing and verification of data. Later data is send to the base station.

Key update

Cluster head can update their key when cluster member attempts to change the cluster. That node considered as malicious node.\

Key revocation

Revocation of a key for a node is performed when a node is reintroduced in a cluster or when cluster head sense come malicious activity in a cluster.

Addition of New Node

The new node generates public/private key through the node generation phase.

B. Algorithm

The different algorithms used in our system are described below.

Algorithm 1: Proposed Algorithm

1. Generate a network graph as Graph g (v) where; V is vertices/nodes.

2. Apply clustering algorithm on the number of nodes and divide the nodes in to number of clusters.
3. On The basis of energy, the base station selects the Efficient Cluster Head.
4. Each node shares unique individual key with Base Station.
5. Each node shares dissimilar pairwise key with each of its neighboring nodes.
6. All nodes in a cluster share a key known as a cluster key.
7. Perform the route generations from each node to the cluster head.
8. Execute the route generations from each node to the base station.
9. Generate the data at each node.
10. Send the individual data to the cluster head from each cluster member in all the clusters.
11. Gather all data at the cluster head.
12. Aggregate all the data and send this data to the base station.
13. Base station accepts the data from each cluster head.

Algorithm 2: ECC Algorithm

The Elliptic Curve Cryptographic (ECC) Algorithm followed by following steps:

Key Generation:
1. Generate public key (pk) and secret key(sk) for all nodes in network.
2. Select number of d range up to n.
   d: it is the secret key.
3. For generation of public key:
   $Q = d * p$;
   d: selected random number;
   p: point of curve

Message Encryption:
1. Generate two cipher text:
   $C1 = k * p$;
   $C2 = M + k * Q$
   k: Randomly selected number
   p: Secret key
   M: Original message
   Q: Public key

Message Decryption:
1. Received Message:
   $M = C2\text{-}d * C1$;
   C1, C2: Cipher text
   d: Random number

Algorithm 3: HEED Algorithm

Pseudo code of HEED Protocol is,
Step 1: V= Set of all nodes
Step 2: Initialize energy to each node of V.
Step 3: Calculate energy of each node N.
Step 4: Compare energy of all nodes.
Step 5: Select maximum energy node.
Step 6: CH = node who's having maximum energy.

A. Mathematical Model

System S is represented as S = {N, B, C, CH, IK, PK, CK, F}

1. Deploy nodes
   N= {N1, N2, ... , Nn}
   N is set of all deployed nodes.

2. Create Base Station
   B= {B1, B2, ……,Bn}
   Where, B is a set of all base stations.

3. Create clusters
   C= {C1, C2, ...,Cn}
   Where, C is a set of all clusters.

4. Select the Cluster Heads in Each Cluster
   CH = {CH1, CH2,....,CHn}
   Where CH is a set of all cluster head.

5. Generate the individual keys for authentication
   IK = {IK1, IK2,....,IKn}
   Where IK is a set of all Keys.

6. Generate the Pairwise keys for authentication
   PK = {PK1, PK2,....,PKn}
   Where PK is a set of all Keys.

7. Generate the Cluster keys for authentication
   CK = {CK1, CK2,....,CKn}
   Where CK is a set of all Keys.

8. Send the data from cluster members to cluster Head and from here to base station
   F = {F1, F2, F3, ..., Fn}
   Where, F is a set of all data files transmitted.

IV. RESULTS AND DISCUSSION

Experimental Setup

The above system is generated using Java framework-version jdk 8 on Windows platform. Development tool used is Netbeans version 8.1. Jung tool generates

network. Modular machine is capable of running the application.

Results

A. Energy Consumption Graph

The fig. 2 and fig. 3 shows the energy and time comparison graph between existing and proposed system. The proposed system consumes less energy and time than the existing system. It enhances the network lifetime and improves the performance.

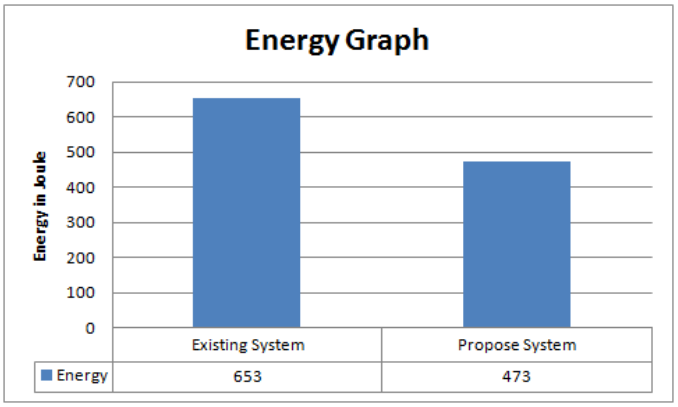

Fig.2 Energy Comparison between Existing and Propose System

B. Time Graph

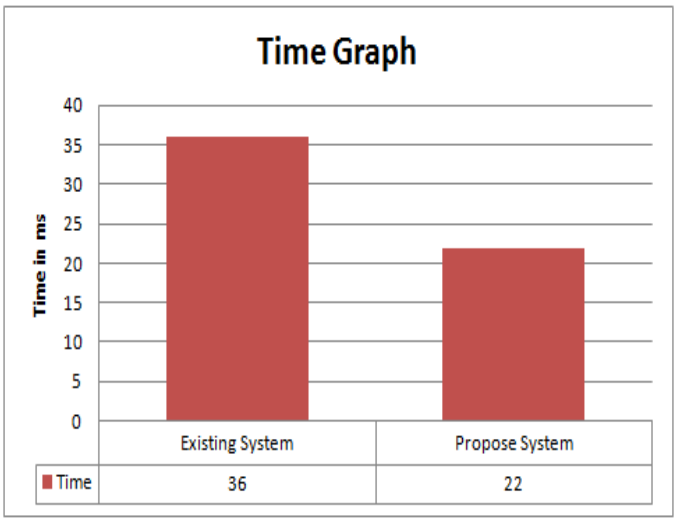

Fig 3. Time Comparison between Existing and Propose System

V. CONCLUSION

In this paper, we propose the HEED protocol for cluster head election in cluster to increase energy efficiency and to increase the network lifetime in wireless sensor network. Our System also proposed to detect malicious data injection from attacker on cluster members and cluster head for secure communication and authentication in wireless sensor network. We also proposed sub base station scheme to reduce the overhead on base station.

In future, energy aware routing will be introduced by calculating shortest path from each sensor to the base station in wireless sensor network with a mathematical model for the system will introduced.

REFERNCES

[1] 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] 2. 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.

[3] 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.

[4] 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.

[5] Ablolfazl Afsharzadeh Kazerooni, Hamed Jelodar, Javad Aramideh, “LEACH and HEED Clustering Algorithm, A Quantitative Study”, in Advances in Science and Technology Research Journal Volume 9, No. 25, March 2015, pages 7-11,DOI:10.12913/22998624/1918.

[6] Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, Fellow, IEEE, “Effective Key Management in Dynamic Wireless Sensor Networks”, in IEEE Transaction on Information Forensic and Security, Vol. 10, NO. 2, Feb 2015.

[7] M.R. Alagheband M.R. Aref, “Dynamic and secure key management model for hierarchical heterogeneous sensor networks”, Published in IET Information Security Received on 2nd December 2011 DOI: 10.1049/iet-ifs.2012.0144.

[8] Ching-Tsung Hsueh, Chih-Yu Wen, Member, IEEE, and Yen-Chieh Ouyang, Member, IEEE, “A Secure Scheme

Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks", in IEEE SENSORS JOURNAL, VOL. 15, NO. 6, JUNE 2015.

[9] Jenq-Shiou Leu, Member, IEEE, Tung-Hung Chiang, Min- Chieh Yu, and Kuan-Wu Su, "Energy Efficient Clustering Scheme for Prolonging the Lifetime of Wireless Sensor Network With Isolated Nodes", in IEEE communication letters , Vol. 19, NO. 2, Feb 2015.