International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 6, May 2016

ISSN: 2394-4404

Providing Secure And Efficient Communication In WSN Using Key Management

Trupti Mujumdar

M. Tech, Student,
Digitial Communication and Networking,
Department of Telecommunication Engg.,
Dayanand Sagar College of Engg.,
Bangalore

Mrs. Srividya B.V

Assistant Professor,
Department of Telecommunication Engg.,
Dayanand Sagar College of Engg.,
Bangalore

Abstract: ***Key Management in Wireless Sensor Network (WSN) has many goals which includes the protocol must establish a key between all sensor nodes that must exchange data securely, Node addition and deletion should be supported, Unauthorized nodes should not be allowed to establish communication with network nodes. In this paper we have developed a wireless sensor network to achieve these goals. Our proposed key management system uses RSA for pair wise key generation, Hash method for individual node key generation and distribution. The security analysis shows that the scheme within this paper meets the unique security and efficiency needs of the sensor networks.***

Keywords**:** ***Key Management, WSNs, k-means clustering, RSA, Pair wise, Hash method.***

I. INTRODUCTION

Sensor network is composed of a large number of small, low-cost, low-power devices sensor nodes .Each sensor nodes have many functionality like communicate on short distances,sense environmental data, Perform limited data processing .Network usually also contains "sink" node which connects it to the outside world. Wireless sensor networks (WSNs) have been extensively used in various applications, such as homeland security, battlefield surveillance, environmental monitoring, and health care. Through collection and processing of the sensing data from the coverage area, WSNs enable users to access detailed and reliable information at any time and any place, which is a ubiquitous sensing technology.

Security researches of WSNs mainly focus on key distribution, secure routing protocols, secure transmission, and security defense. In these scopes, using key management mechanisms to settle security issues under the wireless sensor network environment is the most crucial and challenging problem .Main security threats in WSN are Radio links are insecure – eavesdropping / injecting fault information is possible, Sensor nodes are not temper resistant – if it is compromised attacker obtains all security information. Attacker types: Mote-class: attacker has access to some number of nodes with similar characteristics / laptop-class: attacker has access to more powerful devices outside inside: attacker compromised some number of nodes in the network.

Sensor networks must arrange several types of data packets, including packets of routing protocols and packets of key management protocols. The key establishment technique employed in a given sensor network should meet several requirements to be efficient. These requirements may include supporting in-network processing and facilitating self-organization of data, among others. However, the key establishment technique for a secure application must minimally incorporate authenticity, confidentiality, integrity, scalability, and flexibility.

One of the challenges in developing sensor networks is to provide high-security features with limited resources. Sensor networks cannot be costly made as there is always a great chance that they will be deployed in hostile environments and captured for key information or simply destroyed by an adversary, which, in turn, can cause huge losses. Part of these

cost limitation constraints includes an inability to make sensor networks totally tamper-proof. Other sensor node constraints that must be kept in mind while developing a key establishment technique include battery life, transmission range, bandwidth, memory, and prior deployment knowledge.

We classify key management schemes in wireless sensor networks as follows: 1) Single Network-Wide Key, 2) Pair wise Key Establishment, 3) Trusted Base Station, 4) Public Key Schemes (Elliptic Curve Cryptography) , 5) Key Pre distribution Schemes ,6) Dynamic Key Management , and 7) Hierarchical Key Managements etc. The key establishment technique employed in a given sensor network should take into consideration all the requirements, constraints, and evaluation metrics discussed. In our work we have assessed different types of key establishment techniques, each ranging in efficiency by providing various necessary characteristics. In our proposed system we use pair wise and cluster keys for generation and distribution.

II. RELATED WORK

SachinDilip Babar et.al [1], proposed key management and maintenance techniques are defined using cluster based mobile key management scheme with static Cluster Head (CH).The available key management algorithm is efficient in terms of security, but it is not scalable enough to the changing conditions of network and do not work efficiently under node mobility. This method shows less computational overheads, energy consumption and delay as compared with state-of-art solution. The mobility management is difficult when using static cluster head.

Golsorkhtabaramiri et.al [2], explains a new energy efficient hierarchical clustering algorithm shows the performance of clustering algorithm based on soft threshold and member bounds for Wireless sensor networks using different clustering protocols. This algorithm has better performance in CH election and energy efficient. The hierarchical clustering algorithm also improves the lifetime and the energy consumption significantly in the wireless sensor networks. But this scheme is not scalable enough when the changing condition of network.

Zhang, X et.al [3], describes the energy efficiency is essential requirement for wireless sensor networks. The energy efficient deterministic key management (EDDK) scheme is focuses on establishment and maintenance of pair wise keys and local cluster keys. The EDDK scheme is using the elliptic curve digital signature algorithm for both new and mobile sensor nodes can join or rejoin a sensor network securely. In this scheme is the energy consumption and overhead is very low. But this scheme is not scalable for large networks.

III. PROPOSED SYSTEM

Figure1 shows the flowchart of our proposed system. It mainly includes.

A. CLUSTER FORMATION

The operation of a sensor network starts with the cluster set up phase, in which clusters of the sensor nodes are formed, followed by the data transmission phase, in which cluster nodes will transmit the collected data to cluster head (CH). Each cluster head aggregates the data received from cluster nodes and relays to the base station. The cluster set up phase is divided into two sub clustering phases. In first sub clustering phase, the base station has to cluster the sensor nodes and assign the proper roles to them. In second sub clustering phase, if the energy of the cluster node is getting down it will try to find out the better cluster head.

- ✓ BS will arbitrarily chooses k nodes as initial cluster heads having maximum energy and closer to the node
- ✓ Repeat
- ✓ (Re) assign each node to the cluster with the nearest CH.
- ✓ Calculate the mean value of the Cluster.
- ✓ Until no change.

B. INDIVIDUAL KEY

Individual key is a unique key of each sensor node that shared with the controller (the base station) which is used for individual authentication and secure communication assurance. First of all, it is argued that each node holds the key establishment function *f* and an initial key k which is derived from the master key k that is only possessed by the controller;

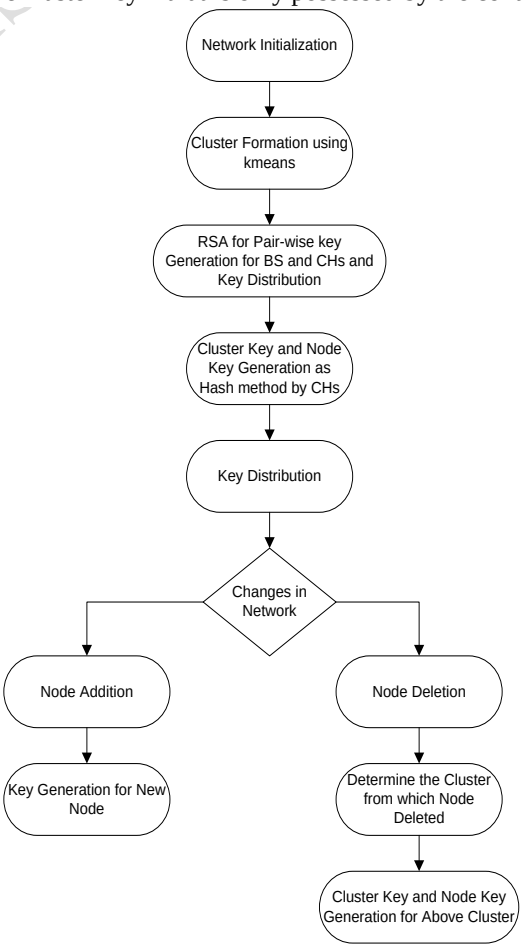


Figure1: Shows the Flowchart of our proposed system

$$K_A = f(K_I, A) \quad (1)$$

In the above, the function f for key establishment is a pseudorandom function and it is efficient enough to be used on sensor nodes.

C. PAIR-WISE AND INDIVIDUAL NODE KEY GENERATION USING HASH FUNCTION

Each cluster has a head node (H) which communicates wirelessly with its nodes, each sensor nodes generate the individual key sets which are then used to generate the common pair-wise key for any two nodes wishing to communicate. This 2 approach makes sure that no two nodes can have any keys in common. The pair-wise key generation scheme has two steps: (a) deployment of sensors and individual key generation by nodes and (b) authentication of sensor nodes and generation of pair wise key.

- ✓ *RSA algorithm* is used for authentication it includes following steps
  - RSA (Rivest, Shamir and Adleman) uses public key and private key to encrypt and decrypt messages.
  - RSA public keys are generated using 2 large prime numbers.
  - RSA public key security is based the difficult level of factoring prime numbers. Given P and q to calculate

$$n = p * q \quad (2)$$

  - But given n to find p and q is very difficult.
- ✓ *Hash function*

The concept of hash function used is defined as:

SHA-256 operates in the manner of MD4, MD5, and SHA-1: The message to be hashed is first

- padded with its length in such a way that the result is a multiple of 512 bits long, and then
- Parsed into 512-bit message blocks $M^{(1)}, M^{(2)}, M^{(3)}, \ldots, M^{(N)}$.

The message blocks are processed one at a time: Beginning with a fixed initial hash value $H^{(0)}$, sequentially computed as

$$H^{(i)} = H^{(i-1)} + C_{M^{(i)}}\left(H^{(i-1)}\right), \quad (3)$$

Where C is the SHA-256 compression function and + means word-wise mod $2^{(32)}$ addition. $H^{(N)}$ is the hash of M.

H generates its key using hash function h and passes it to the next node of the cluster. The key generation continues until the last node of the cluster has generated its key. Since key generation is hash chain based, only H has the ability to generate individual keys for any node in its cluster as it knows the location of all the nodes in its cluster.

D. NODE DELETION

Node deletion In WSNs, it is necessary to preserve the shared keys secrecy when a node is compromised, thus avoid the number of compromised nodes reached a critical value. When new node delete, CH broadcasts a notification to its cluster members and removes the compromised node from its cluster member table. If a CH is compromised, a re-clustering of cluster member of the compromised CH among the remaining CH needs to take place.

.

E. NODE ADDITION

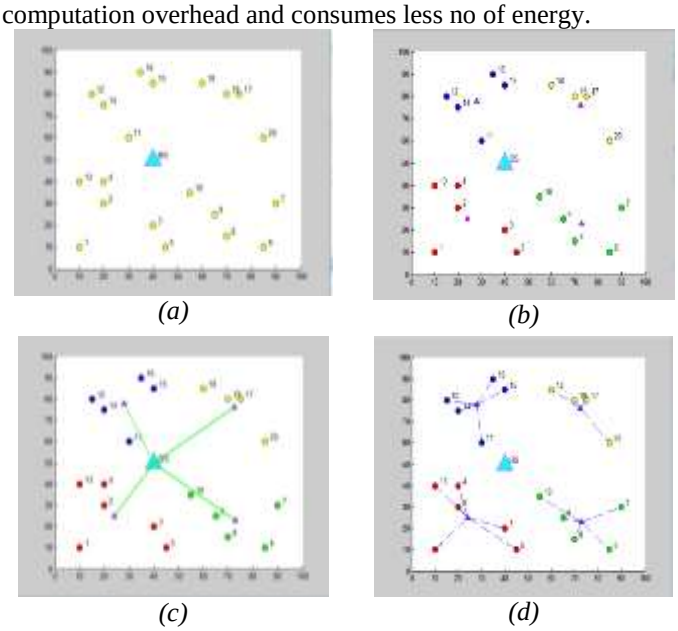
Node addition If a new node is added in the network, the BS after authentication process assign the new node in a group and loads it with the unique secret shared. The BS notifies the CHs about the new node's arrival. Then, CHs send an advertisement message adv. Once receiving requests from CHs, new node selects one of the CHs as its own CH, based on some parameters such as the strongest signal received from a CH.

IV. RESULTS

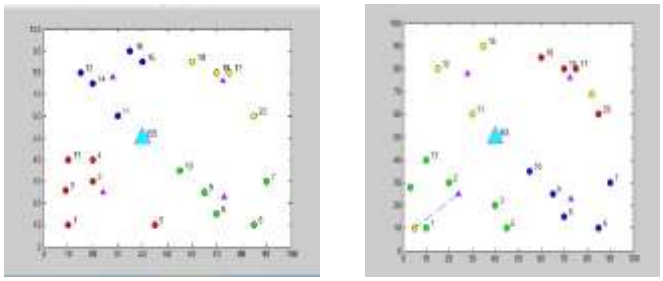
In this section explains the proposed system step-by-step output of all the phases and graph plot comparison with the existing methods.

Figure 2(a) shows Network initialization with wireless sensor networks which wish to communicate, in second step cluster formation using k-means algorithm to for different clusters and to identify cluster head(CH),which is shown in figure 2(b)here each individual colors represents different clusters. In third step, pair wise key generation between base station (BS) and each cluster head (CH) takes place as shown in figure 2(c). In fourth step node key generation i.e., individual node key generation and distribution using hash method is displayed in figure 2(d).next step explains node addition and node deletion in figure 2(e) &2(f), after node is added to the network successfully a prompt appears shown in figure 2(g), similarly after node deletion a prompt appears as shown in figure 2(h).

As the next part of experimental results, graph plot between our proposed method and existing method. Is shown below, in both the graphs our proposed system has less computation overhead and consumes less no of energy.



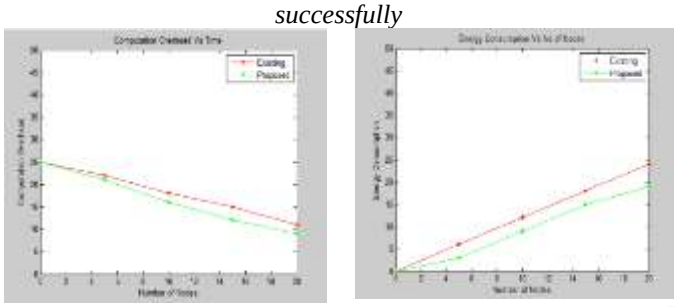
(a) *(b)* *(c)* *(d)*



(e) *(f)*

(g) *(h)*

Figure 2: (a) Network Initialization, (b) Cluster formation, (c) Pair wise key generation, (d) Nodes key generation,(e) key deletion in cluster (f) key addition in cluster, (g) prompt for key deleted successfully(h) prompt for new key added successfully



(a) *(b)*

Figure 2: shows the experimental results plotted using graph (a) computation overhead vs. time. (b) Energy consumption vs. no. of nodes

V. CONCLUSION

This paper proposes a pair- wise and individual node key management scheme for wireless sensor networks. It supports the establishment of pair-wise keys and cluster keys to enable different communication patterns. Use of Pair-wise keys provides node-to-node authentication and resilience to node replication. Use of clustering reduces the energy consumption of nodes and lengthens the network lifetime. Which is proven in experimental results compared to the existing methods our proposed method consumes less engery.Use of pair wise key management gives robustness.

REFERENCES

[1] SachinDilip, "Cluster-based mobile key management scheme for wireless sensor network", Emerald Group Publishing Limited ,International Journal of Pervasive Computing and Communications, Vol. 10,pp. 1742-7371, 2014.

[2] Golsor khtabaramiri M, "HCABS: The hierarchical clustering algorithm based on soft threshold and cluster member bounds for wireless sensor networks". IEICE Electron Express, Vol. 7, pp. 685– 690, 2012.

[3] Zhang, X.,"EDDK: Energy-Efficient distributed deterministic key management for wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, Vol.5, no.1, 2012.

[4] Kausar, "Scalable and efficient key management for heterogeneous sensor networks of Supercomputing", Vol. 45, No. 1, pp. 44-65, 2008.

[5] Chan, "Random key pre distribution schemes for sensor networks", Proc. of IEEE Symposium on Security and Privacy, pp. 197-213, 2003.

[6] D. Huang, "Location-Aware Key Management Scheme for Wireless Sensor Networks," in Proc. of ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'04), pp. 29-42, Oct. 2004.

[7] Z. Ming, W. Suo-ping, and X. He, "Dynamic key management scheme for wireless sensor networks based on cluster," Journal of Nanjing University of Posts and Telecommunications (Natural Science), Vol. 32, No. 1, 2012.

[8] Y.-F. Ciou, "A handover security mechanism employing the Diffie-Hellman key exchange approach for the IEEE802.16e wireless networks," Mobile Information Systems, Vol. 7, No. 3, pp. 241–269, 2011.

[9] J. Li, Q. Wang, C. Wang, and K. Ren, "Enhancing attribute-based encryption with attribute hierarchy Mobile Networks and Applications", Vol. 16, No. 5, pp. 553–561, 2011.

[10] Y. S. Lee, J. W. Park, and L. Barolli, "A localization algorithm based on AOA for ad-hoc sensor networks, Mobile Information Systems", Vol. 8, No. 1, pp. 61–72, 2012.