ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 7, July 2016

Improved Security in Wireless Sensor Networks using Encrypted Key Distribution Techniques

Rachana Srivastava[1], Neha Sawal[2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & NGF College of Engineering &Technology Palwal, Haryana, India

Abstract: **The evolution of wireless networking as well as the growth in embedded systems and techniques have provided birth to application specific networks known as wireless sensor networks WSNs, their reliability, facility of usage and deployment as well as their low cost provide them an increasing area of applications. Often sensors are restricted in capabilities deployed in a unpredictable and hostile atmosphere, building the security of these networks a major issue. In this paper, it is introduced a dynamic key management system for Wireless sensor networks with the cluster head as a coordination center and key distribution for asymmetric keys. Public keys of the sensor nodes are dispatched by cluster head and symmetric keys set with these key combinations.**

I. INTRODUCTION

A wireless sensor network consists hundreds to thousands of small, low power, low cost and multifunctional sensor nodes, having the probability to sense and gather application-specific data i.e. pressure, temperature and movement to permit atmosphere monitoring [1, 2]. Because of their services and deployment flexibility, ad hoc connectivity as well as the autonomy and the cheaper sensors, wireless sensor networks are involved in various areas ranging from the military applications i.e. battlefield surveillance [3], to civilian ones involving atmosphere and habitat monitoring, home automation, healthcare applications, environmental monitoring, traffic control or to detect and characterize biological, Chemical, Radiological and Nuclear in some atmosphere where the existence of human is not possible[4]. Wireless sensor networks are very usual part of hostile and unpredictable atmosphere, often exposed to several attacks and risks. Thus, the aspect of security must take the higher attention to secure the network from the increasing no. of attacks against WSNs, under the restrained behavior of sensors, often restricted in energy and computing power which builds the traditional security techniques waste for WSNs.

II. SENSOR NETWORK ARCHITECTURES

In a WSN, sensors are very usually dispersed in a large area often without any centralized management for maintaining the network architecture and set up connectivity from end sensors to the BS; thus sensors must cooperate among themselves to set up this connectivity without the support of any administrative authority. Classically, two main architectures are available for WSNs the hierarchical and the flat network architectures [6].

2.1 Flat Network Architecture

In flat network architecture, all nodes are equal in roles and links are established directly between nodes and the BS, in the way that data is forwarded from sensors to the BS such as any other ad hoc network. Sensors utilize conventional routing to set up end to end link with the BS. Flat networks are very appropriate for stable sensor network where the gathered reports are not multiple, which do not add a high overhead to the network for their transmission to the BS. Since, routing in this architecture utilizes broadcasting which uses lot of network resources and occasionally network overhead.

2.2 Hierarchical Network Architecture

In a hierarchical architecture, sensors are partitioned into regions or clusters. One node in the cluster is elected as cluster head targeted to maintain the cluster formation and management, other sensors known as cluster members are linked to the closest cluster head. Cluster heads maintain the transmission between base station and sensors which decrease considerably the overhead of network however the gathered data is forwarded to the cluster head which forwarded an abstract report to the BS which decreases the traffic out clusters and thus across the network.

III. SECURITY IN WIRELESS SENSOR NETWORKS

Security is a very significant task when deploying or designing any protocol or network, since the recent developed networks i.e. the wireless ones have not provided the essential attention to security when designing protocols by taking into consideration these networks specificity such as the utilized medium and the devices restraints as well as the deployment environment [7]. In this section, we are going to explain the several key management techniques offered in literature as well as their viability and efficiency for WSNs.

***Shared Key*:** This is the easiest technique to protect any class of network wireless or wired [8]. In this type of techniques one key is shared among all the network nodes. In WSN case, the shared key is preloaded by an offline dealer before the deployment of network. From resources perspective this technique does not add any overhead for key exchange and establishment however the utilized key is recorded in every sensor before deployment also very little computation and storage capacity are required to encrypt and decrypt traffic throughout the network. In the other hands this techniques is very susceptible against cryptanalytic attacks, however a WSN is deployed for long period which builds this class of attacks possible. In addition to cryptanalytic attacks, this technique show a point of failure which is the shared key however the compromising of a single node because of physical attack causes the compromise of the entire network.

Pair-wise Key Establishment: For overcoming the limitations of the prior technique caused by the usage of a single shared key, the pair-wise key establishment aim to share various keys between each sensor pair throughout the network, the employed keys are preloaded before deployment by an offline administrative authority. Thus, for n sensors network, each node records n−1 keys in its memory. After deployment every node sets up a secret key with every one of its neighbors, by viewing for the corresponding key in the pull of keys preloaded before deployment [8]. This technique does not require any computation and communication resources however the keys are preloaded before deployment, since it impose large storage capacities for storing all the possible keys, building this solution inappropriate for large scale networks.
From the security perspective this technique assures a high threshold of security robust against various attacks.

Random Pair-wise Key Establishment: This technique is formulated to overcome the limitations of simple pair-wise key establishment, which requires a significant storage capacity to record all the possible keys. This technique considers that all sensor nodes pair in a WSN do not require a communication path with one another, in the way that a node requires to protect only a sub set of connections [10].
To build this in practice sensors record only a sub set of the key pull described in simple pair-wise key establishment and shares secret key with its neighboring nodes with a provided possibility. This possibility must be selected according to the no. of sensors in the network as well as the required connectivity level, which builds this technique more complicated and does not maintain the network widening efficiently. In comparison of the simple Pair-wise Key Establishment this technique is more effective.

Trusted Key Distribution Center: In the prior key management techniques every sensors shares a secret key with each of its neighboring nodes, for decreasing the overhead because of communication since these techniques are not appropriate for huge networks, because of the restricted sensors storage capacity [11]. Accordingly, the trusted key distribution center technique introduces to decrease the overhead because of key storage by installing a central server responsible of key distribution throughout the network. After the deployment of network every sensor contacts the server to achieve a pair-wise key for each session. This technique is robust against traffic analysis and node capture however the key may be updated periodically. Since, it adds a high communication overhead for pair-wise keys establishment which causes a congestion area around the key server. It also generates a point of failure which is the trusted server against spoofing attacks, however the cloning or spoofing of the server may compromise the entire network

IV. PROPOSED APPROACH

In this section, we show the overall details of our method that assures the following security features:
Forward Secrecy: Even if an intruder retrieved the adjacent Key in the cluster but the extra cluster keys are impossible to retrieve.
Privacy: Even the node is fetched by an intruder; the secret key in the node's memory cannot be recovered.
Data Confidentiality: Data Confidentiality ensures that any attacker or other neighboring system could not achieve secret information intercepting the transmissions.
Our method has three kinds of keys:

Cluster Key: Every sensor node have neighbors' public keys to authorize every neighbor in cluster.
Pairwise Key: For assuring secure interaction to agree on a pair wise session key. KAB offers confidential communication between a cluster head and its cluster member.
Individual Key: Every sensor node has a unique key shared with the center. This key is utilized for secure communication between the center and a sensor node.

V. CLUSTERING TECHNIQUE

Our method considers wireless sensor network in which the nodes are dynamic with similar communication and computational capabilities. The network utilizes Clustering mechanism for secure communication and key distribution. In a cluster, all the nodes manage different keys, but each node utilizes same key for various communications with the base station (BS).Clustering is the technique of organizing objects in to groups whose members are same in some way, where one node in every cluster as cluster head, responsible for some tasks. Clustering offers a mutual organization of sensor nodes that makes easy the coordination of transmission between neighboring nodes. This function decreases disturbance in multiple access broadcast atmosphere. Every cluster contains a cluster head (CH), one or more sensor nodes. The cluster head organizes the transmission of public key for every cluster node, this offers communicate quickly among cluster members, which offers direct communication with a farther node. Additionally, a node moving in the same cluster without overlapping zone doesn't make any issue however it doesn't influence the cluster structure. The clustering process consists of three kinds of nodes: Mobile Certification Authority (an administrator) which will be available only at the initialization step then it can leave the network; a group of cluster head (CH) offers master facilities. Every node has a public and a private key. In the architecture, we assume that every cluster head is a mobile certification authority for its cluster members. To establish a secure WSN system, this decreases resource consumption and increases security performance. Consist of several nodes, which are distributed into a huge area and one (or more) Mobile Certification Authority (MCA) and coordination center of the system.

5.1 Key Preloaded in sensor node

The best key distribution technique is preloading the secret keys into sensor node before they are deployed. Same as, some confidential information required to be pre-loaded into sensor nodes before their deployment. In our introduced technique, sensor nodes are preloaded every with one unique secret key, shared with the other sensor node. Sensor nodes must authorize themselves with the other sensor node utilizing their corresponding unique keys. During this technique, the other sensor node creates ID and loads every node with this key. The ID can be viewed as the network key and will be utilized during the cluster formation procedure. Observe that all members should prove their validity to the sink node. So for every node, a unique key is utilize to authorize the own node, shared with the target sensor node (KAB) and is removed after the first round.

5.2 Neighbors' public key distributed over cluster head

After the cluster establishment, the cluster heads schedule and report every cluster member. The sensor nodes are actively transferring or hearing for a time period and off the remainder. The sensor nodes transfer only at their scheduled time. This permits the sensor nodes to hear to the communication in their corresponding clusters. It is through this passive hearing that the sensor nodes are capable to develop trust relationships with their neighboring nodes. Nodes that constantly discard packets or which act in a selfish or selective way can be easily determined by their neighbors. Every sensor node records and manages a trust key value of its neighboring nodes.

5.3 Secure communication using pair-wise keying

Pair wise keying procedure offers fundamental security facilities in WSNs. That enables sensor nodes to interact securely with one another utilizing cryptographic methods. These bear sensor node compromise by restricting the scope of each key. Hence, a sensor node compromise only influences past and future messages forwarded to or from that sensor node; other traffic is uninfluenced. Higher robustness against sensor node compromise does come at a cost, especially in the overhead included for key management. If a sensor node interacts with a huge no. of sensor nodes, it must record several keys and choose the suitable ones when communicating. However, sensor nodes are restrained in resources, this storage cost included can be prohibitive. This technology offers Pair wise key establishment and management methods which support in making the network protected.

Table1. Diffie-Hellman Key Exchange Algorithm

Public key, Parameter Creation	
A Cluster head chooses and publishes a Prime Public key P and an key c having large prime order in C*P.	
Private key Computations	
Node A	Node B
Choose a secret key a. Compute Node A ≡ ca (mod P)	Choose a secret key b. Compute Node B ≡ cb (mod P).
Public key Exchange of key values	
Node A sends A to Node B → A B ← Node B sends B to Node B	
Further Private key Computations	
Node A	Node B
Compute the key value Ba (mod P).	Compute the key value Ab (mod P).
The shared secret key value is Ba = (cb)a = cab = (ca)b = Ab (mod P).	

VI. KEY DISTRIBUTION AND ENCRYPTION MODEL OF THE SYSTEM

In our introduced technique, clustering is started by sensor nodes. Assume if any two key are process as Node A and Node B are two interacting sensor nodes in the WSN System. MCA is a cluster head inside an ad hoc network, and it is chosen to offer distributed key management center's service. KAB is the communication pair wise keys between nodes A and B. {M} PubA represents the encryption of message M with Public Key of A node.

Step 1 A sensor node (A Node) flood a message, which consist its ID (IDA) to its neighbors.
Step 2 Every neighbor (Node B and others) should get the Public Key of A Node from MCA.
Step 3 Sensor Node B utilizes Sensor Node A's public key to encrypt messages which consist its identifier (IDB) and a random no. (RN1), which is utilized to determine this transaction
Step 4 Sensor Node A forwards a message to Sensor Node B encrypted with PubB and consisting B's random no. (RN1) as well as a new random no. created by Node A (RN2).
Step 5 Sensor Node B chooses a secret key KAB and returns this and RN2, which are encrypted utilizing PubA, to ensure A that its correspondent is B.
Step 6 The interacting parties (Sensor Nodes) are agreeing on a Pair wise key and they can utilize this for secure communication.

Table2. Diffie-Hellman Key Creation, Encryption And decryption

Public key, Parameter Creation	
A Trusted party selects and publishes a Prime Public key P and a key element c modulo p of large prime order.	
Node A	Node B
Key Creation	
Choose Private key 1≤ a ≤ p-1. Computes A = ca (mod p). Publishes the public key A.	
Encryption	
	Choose Plaintext m. Choose random ephemeral key k. Uses Node A public key A to compute c1 = ck (mod p) and c2 = MAk (mod p). Sends

	ciphertext (c1,c2) to Node A.
Decryption	
Compute the key value (c1 a) -1 . c2 (mod p) This key value is equal to M = KAB.	

Table3. Notations

Symbols	Explanation
CH	Cluster Head
BS	Base Station
ID	Identifier of Node
IDA	Identifier of Node A
IDB	Identifier of Node B
PubA	Encrypted value of Node A
PubB	Encrypted value of Node B
K KAB RN MCA	Pairwise key Pairwise key of A and B Random Number Mobile Certified Authority

VII. SIMULATION AND ANALYSIS

This section compares the introduced algorithm performance with skip jack algorithm. The performance measurement involves throughput . The sensor nodes are modeled to deploy over a cluster with adjustable interaction range and static sensing range. Simulation is done utilizing OPNET modeler. We have compared the Clustered Time Synchronization performance with skip jack. The cause is clear that because of clustering the sensor nodes inside the cluster have not to transfer for large distances and message exchange is also very less in comparison of the other that save an important amount of energy. Our introduced process decreases the no. of data exchanges. In Wireless sensor networks, most of the energy is used for transferring and obtaining the data, thus reduction in data exchange also decrease the energy consumption.

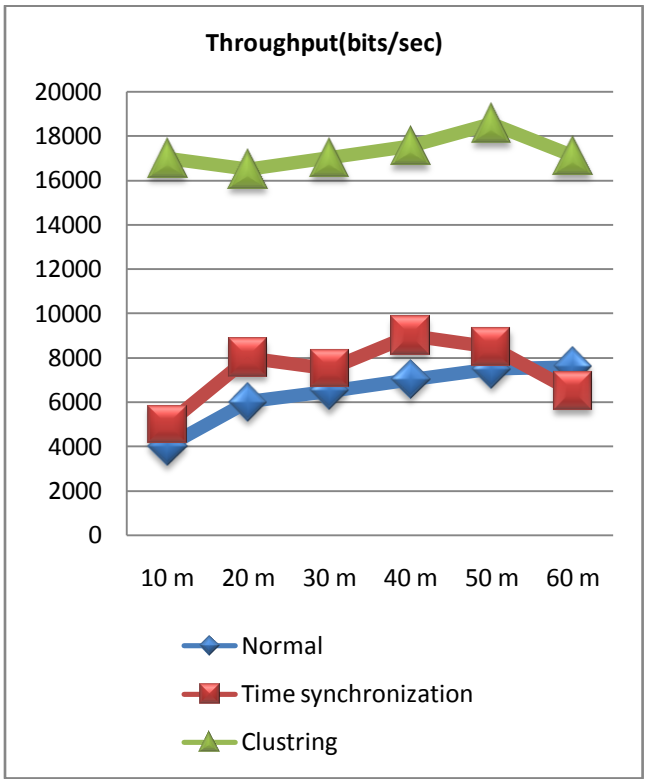

Figure 6. Proposed Approach

CONCLUSION

Cluster for WSN was introduced to synchronize the whole nodes of the entire network. In the cluster process, it followed Pair wise key exchange technique to obtain the time synchronization between the cluster heads and Base Station. In the clustering stage, it followed ID broadcast technique to complete the time synchronization between cluster members and cluster heads. The simulation results represented that the proposed algorithm compared to skip jack algorithm, had high throughput and better synchronization precision. Our method determines the attacks i.e. Dos attack, Reply attack when network is influenced because of pre-distribution of keys to cluster node. To approach these security concerns, it would be required to study the current technological advances in distributed systems.

REFERENCES

[1] Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", International conference on Information, Networking and Automation(ICINA),Kunming, IEEE, pp. 215-218, 2010.

[2] Fan Li and Yu Wang; " Survey of Routing in Wireless Sensor Networks",in Proceedings ofIEEE Wireless Sensor Networks Technology Magazine, Volume 2, Issue 2, June 2007; pp. 12-22.

[3]Gurjot singh, Ram singh , "A Secure Routing Scheme for Static Wireless Sensor Networks", IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol.2, pp.776-780, 2008.

[4] Harpreet Singh, Gurpreet Singh Josan, "Performance Analysis of AODV & DSR Routing Protocols in Wireless Sensor Networks", International Journal of Engineering ,Vol. 2, Issue 5,pp,2212-2216, September- October 2012.

[5] HeissenbüttelM., T. Braun, M. Wälchli, and T. Bernoulli, "Optimized stateless broadcasting in wireless multi-hop networks," in proceeding of 4th IEEE international conference on Infocom Barcelona,2006,pp.234-250.

[6]Hemanta Kumar Kalita and Avijit Kar "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009,pp.3-10.

[7] Jahanzeb Farooq, Bilal Rauf "Implementation and Evaluation of IEEE 802.11e WirelessLAN in GloMoSim" In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.

[8] Julio Lopez and Ricardo Dahab, "Fast Multiplication on Elliptic Curves over GF (2m)without Precomputation", Springer 2009

[9] KorkmazG., E. Ekici, F. Ozgüner, and U. Ozgüner, "Urban multi-hop broadcast protocolforWireless Sensor Networks," In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.

[10] K.S.Arikumar, K.Thirumoorthy, "Improved User Authentication in Wireless Sensor Networks", 2011 IEEE.

[11] Marco Martal`o, Chiara Buratti, Gianluigi Ferrari, and Roberto Verdone "Clustered IEEE 802.15.4 Sensor Networks with Data Aggregation:Energy Consumption and Probability of Error" In Proceedings of IEEE Wireless Communication ,VOL. 2, 2013, pp 23-45.

[12] Rajive Bagrodia, Richard Meyer, Mineo Takai, Yu an Chen, Xiang Zeng, Jay Martin, andHa Yoon Song. "A parallel simulation environment for complex systems"in Proceedings of the 1st ACM international workshop on ad hoc networks; 2004; Pages: 66 – 75.

[13] Rayala Upendar Rao, "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys", International Journal of Computer Applications, Vol. 55, Issue. 7, pp.48-52, October 2012.

[14] R.Balasubramaniyan , Dr. M. Chandrasekaran "A New Fuzzy Based Clustering algorithm for Wireless MobileAd-Hoc Sensor Networks"In Proceedings of 2013 International Conference on Computer Communication and Informatics,2013, pp 31-37.

[15] R.U.Anitha, P. Kamalakkannan ,"Enhanced Cluster Based Routing Protocol for MobileNodes in Wireless Sensor Network" In Proceedings of 2013 International Conference onPattern Recognition, Informatics and Mobile Engineering (PRIME), 2006,PP 187-193.

[16] Ritu Sharma, Yogesh Chaba & Yudhvir Singh, "Analysis of Security Protocols in Wireless Sensor Network", International Journal Advanced Networking and Applications Vol02, Issue 03, 2010, pp. 707-713

[17] Sahabul Alam and Debashis De, "Analysis of Security Threats In Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Vol. 6, No. 2, April 2014, pp 35-46."

[18] Dr. Salim Ali Abbas and Amal AbdulBaqiMaryoosh, "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography**",** IOSR Journal of Computer Engineering (IOSR-JCE), Vol 17, Issue 4, Ver. I, July – Aug. 2015, pp 48-53.

[19] Samera. B. Awwad, cheekyunng and Nor K. Noordin "Cluster BasedRouting (CBR) Protocol with Adaptive Scheduling for Mobility andEnergy Awareness in Wireless Sensor Network," *In Proceedings of Proceedings of theAsia Pacific Advanced Network*,2009, pp 34-46.

[20] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, Wireless Communication and Mobile Computing, Vol. 4,No 6,pp.623-637,2009.