A Study on Secure Data Transfer in Cluster-based Wireless Sensor Networks

Anil Kumar K, Latha.A

Abstract*—Transmission of data securely is a severe issue to accomplish an improvement for wireless sensor networks (WSNs). The much effective approach to improve the system overall performance of Wireless Sensor Networks is via clustering. We learn the secure data transmission for cluster-based WSNs (CWSNs); here the clusters are formed with using modular function for electing cluster head. We propose secure data Transmission protocols for CWSNs, called Signature based offline/online signature to minimize the overhead for data transmission in the protocol security for faster computation, which is very much important for WSNs. For data transmission we propose the algorithm secure offline/online signature in the existing they have used secLEECH. They future results are provided to illustrate the efficiency of proposed protocols. The results shows for the proposed protocols have much more performance than the existing protocol scheme for CWSNs, in terms of energy consumption and security overhead.

***Index Terms*— Cluster-based WSNs, signature-based online/offline digital signature, efficient data transmission, SNR (signal to noise ratio)**

I INTRODUCTION

In this modern world we thrive in using technology which is the most effective and easier in terms of viewing, scanning and to process the obtained data. Wireless sensor network is becoming a vital part in such activities. The wireless sensor network comprises of node which interfaces with nodes that scan the environment which are sensor nodes, and as the name depicts "wireless", the obtained data is transmitted wirelessly to the base station which acts as a repository. Wireless sensor network (WSN) refers to a group of nodes working in a spatially dispersed environment and set of specific dedicated sensors for observe and check the progress of several applications and recording the physical conditions of the environment and arranging the collected data at a central location. addressed. Energy consumption can be constrained through clustering.

***Anil kumar k**, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*
***Latha.A**, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*

WSNs measure environmental conditions [1]. The more modern networks are multi directional and enabling control of sensor activity. One of the major threats in wireless sensor network is security and huge consumption of energy which has to be the innovation of wireless sensor networks was motivated by establishment of many military applications, nowadays these networks are used in many industrial areas and consumer applications. The more secure and effective method of data transmission is main issues for cluster based wireless sensor network, many WSNs are found in noise, avoided and often involving by conflict or opposition in physical environments for certain applications, such as sensing predefined method and an area of territory with trust less surroundings. WSNs are expected to be solutions to many applications, such as tracking the location of personnel in a building and detecting, measuring traffic flows on roads, monitoring environmental pollutants, and tracking the passage of troops and tanks on a battlefield,. Many sensor networks have mission-critical tasks and thus require that security be considered. Improper use of information or using forged information may cause unwanted information leakage and provide not accurate results. [2].

They are also responsible of sensing environment and information of transmission. The transmission task is crucial issue since there are large amount of data and sensors devices are restricted to a certain level. As the sensor devices are limited to the network that is exposed to variety of attacks. Conventional mechanisms for security are not suitable for WSNs as they are usually heavy and nodes are limited. In a cluster-based WSN (CWSN), every cluster has a cluster head with in sensor node. A ClusterHead combines the information collected by the within a cluster nodes i.e non ClusterHead sensor nodes in its cluster, this data are combined and sent to the base station (BS) [3]. Secure and efficient data transmission is thus required in cluster based wireless sensor network

The Secure offline online signature has a protocol initialization existing to the network the communication is done in particular time for each rounds is predefined. Secure offline online signature has four types of operations, initially extraction, offline signing, online signing and verification. Sensor nodes forward the collected data to the ClusterHeads in steady state phase. For the fair consumption of energy and cluster head

elected based on its energy in that particular round and all the other non-Cluster Head sensor nodes join clusters using single hop transmission.

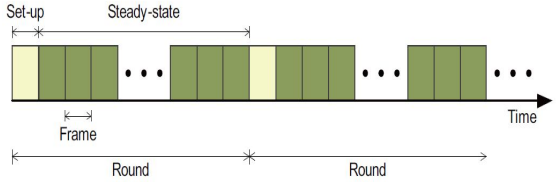


Fig 1. Operation of data transmission

II. LITERATURE SURVEY

The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman et al. [4] the symmetric key scheme to provide the security of information, There are various transmission of data protocols schemes such as LEACH, This protocols provides the data transmission based on SecLEACH, GS-LEACH and RLEACH. The prior scheme used to approach of the symmetric keys to provide the security by adopting this scheme, which has a drawback with the orphan node problem [5]. The orphan node creates a problem which that do not share a pairwise key with other node which leads to LEACH problem in a preloaded ring with a set of keys, which intern leads to increase in number of CHs..

For developing online/offline signature schemes was introduced by Even et al [6]. Multi signatures for AODV and Practical ID-based signature [7-8] are based on online/offline signature schemes however the offline signature in these particular schemes the id are precomputed and they are not worthy suitable for CWSNs.

Another method to reduce the energy-consumption is using different methods of Routing techniques. The data which have been sensed by the sensor nodes are routed to the base station by some strategy which will reduce the energy consumption to a great extent. Routing in Wireless Sensor Network has three classification and they are

1. Flat-based routing – are the nodes where all nodes have equal functionality within the network
2. Hierarchical-based routing – these nodes have different functionality within the network
3. Location-based routing – depends on the position of the nodes within the network that decides the node functionality.

III. ARCHITECTURE

Sensor nodes are combined into individual clusters, and each set of cluster has a cluster-head (CH) sensor node, The non cluster head nodes i.e sensors nodes join's a particular cluster head depending on the distance of near cluster head and receiving signal strength and the each sensor node transmit the sensed data to the BaseStation via ClusterHeads to minimize energy consumption as shown in fig 3.1.

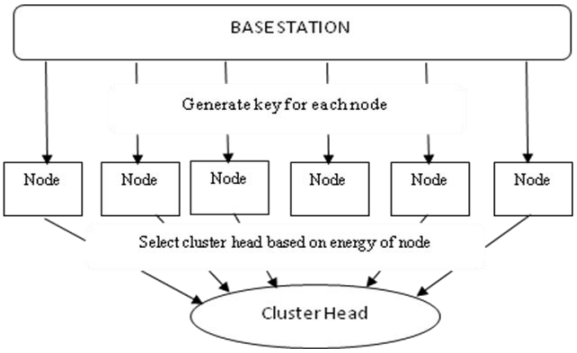


Fig 3.1 - cluster head formation

The architecture shows that initially base station generate id for each node and provides with secret key using AES by using homomorphic encryption algorithm. The cluster head is formed based on the energy of node by calculation the threshold value if the energy is greater than threshold then that node is elected as cluster head for initial round.

The below figure 3.2 shows the cluster head send join request to nearest neighbour for joining the cluster head node elects the cluster by nearest distance to join cluster head after joining cluster head, Cluster head sends the offline signature, time stamp to each of the node joined to that cluster head.

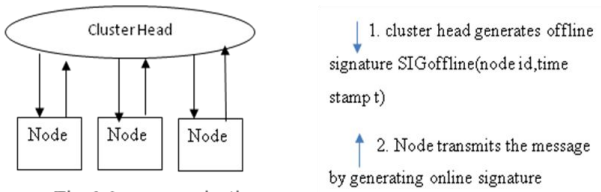


Fig 3.2- communication between cluster head and nodes

The node sends the data to cluster head along with offline signature by encrypting it this data at the cluster head decrypts and verify the offline signature if verification success then the data is sent to base station as shown in figure 3.3 else the node is marked as intruder and blocked it for that particular round

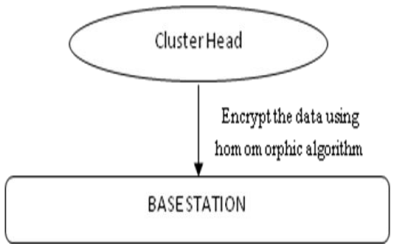
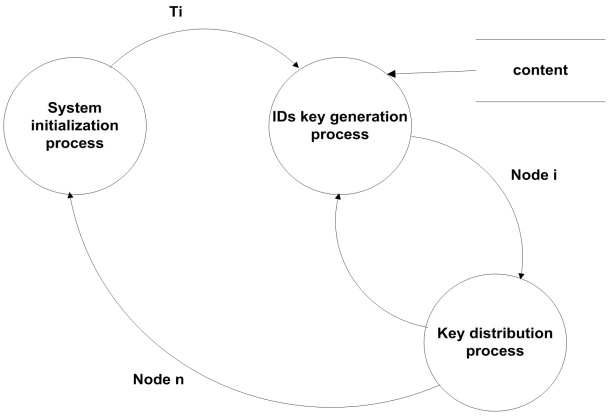


Fig 3.3-Data transmission from cluster head to Basestation

IV. PROTOCAL FRAMEWORK

- Time based system parameter initialization
- Cluster head selector module
- Data upload manager

- **Time based system parameter initialization:** This module is used by the base station to deploy the sensor nodes with the system parameters like Secret Key for data encryption and IDS for the nodes in the network.



- **Cluster head selector module:** Each node runs this module to identify its residual and energy and elect himself as the cluster head and generate signature keys and offline signature to be distributed to the sensor nodes.

- **Data upload manager** Each node generated data and online signature and upload the data to the cluster head. Cluster head runs this module to verify the online signature and upload the data to the base station.

V. PROPOSED METHODS

The proposed scheme helps in transferring the data securely with effective performance methodology than the prior protocol scheme for CWSNs

a. Energy based CH selection

Every Cluster group can elect its own cluster head based on its energy. Among, all the nodes in the cluster, the node, which is having the highest energy, have been chosen as CH. The next highest energy node is chosen as next CH, so that during the next iteration if the CH losses its energy the next CH becomes the Current CH. The threshold defined in equation 1.

$$T_i(n) = \frac{(P \times C)\,(U_i - d(n,BS))}{(1 - P)\,(r \bmod 1/P)\,(U_i - L_i)} \left[\frac{E_{cur}(n)}{E_{min}(n)}\right] K \quad \text{.....(1)}$$

Where
P is the desired percentage of the cluster heads.
r is current running node.
Z is the number of nodes, which are not elected as CHs in the last **1/P** rounds.
C is constant between 0 and 1. Ui is upper limit of level-i, Li‘ is the lower limit of level-i.
d(n, BS) will be the total distance between node n and BS.
Ecur (n) is defined as the current energy of node n.
Emin (n) will be the initial energy of node **n** and the value of **K** will be between zero to three.

b. SNR(signal to noise ratio) based CH selection by NCH nodes

Now the normal node becomes a 1- hop node. It will create its own ID and send a state message to its neighbors within their region. If a Non Clustered Head (NCH) node receives a state message from a 1-hop member node, it will declare itself as a 2-hop member node. The two-hop member node also chooses its own ID, which is **m** byte random integer added at the end of the selected 1-hop member node‘s ID. It may rarely happen that two sensor nodes within a same cluster choose the same random number. This conflict can be solved through the cluster head by giving each nodes a different ID for every round. Hence, at the end of this phase every node has its locally unique ID and knows which cluster it belongs. The abdicate message is sent by each cluster head to notify its member nodes of its unwillingness to serve as the cluster head in the next round, because of their lower energy levels.

c. Data forwarding through Inter cluster routing

After that, each cluster head creates a TDMA schedule for each cluster nodes for each round. The information related to the cluster head will be broadcasted back to the nodes in the cluster and the clusters are created and TDMA for each round is allocated further data transmission is started in that round. Each cluster node can be turned off until the node's allocated time. Each node sends data to its cluster heads with much less consumption of energy in every round. The total energy for transmission of data is estimated by received signal strength of the advertise message, so that transmission of data uses a minimal amount of energy. The cluster head performs the data aggregation function to compress the data into a single signal once all the required data is received from the respective cluster members.

After a certain time the next round, begin. After the formation of cluster, the cluster heads broadcast the data by aggregates them to the further level. At the beginning of next level where the data is aggregated by nodes and sends to their cluster heads. In this particular way, the cluster heads at the last level transmit the final information to the BS.

d. Identifying the intruder

Generally, the attacked area may contain many nodes and the intruder nodes are not necessarily located at the center of the area in a multi-hop sensor network. Hence, it is necessary to further locate the exact intruders and isolate them from the network. This can be achieved through analyzing the routing pattern in the affected area. The proposed method for collecting information that flows with in a predefined network which provides facility for the routing pattern analysis. First, the Base Station (BS) sends a request message to the network. The message contains the IDs of the affected nodes, and is flooded hop by hop. For each node receiving the request, if its ID is there, it should respond to the BS with a message with its ID and the ID of the next-hop node, the cost for every routing is calculated for example the hop-count from the BS. In the next-hop the cost could already be affected by the attack, hence causing the response message should be transmitted along the reverse path in the flooding that corresponds to the original path with no effect intruder.

Operation of Setup phase

Step 1. BS $\Rightarrow G_s$: $< ID_{bs}, T_s >$ /* The BS base statiion broadcasts the information to all nodes. */

Step 2. $CH_i \Rightarrow G_s$: $< ID_i, T_s, adv, \sigma_i, z_i >$ /* The elected ClusterHead broadcast their information. */

Step 3. $L_j \rightarrow CH_i$: $< ID_i, ID_j, T_s, join, \sigma_j, z_j >$ /* A leaf node joins to a cluster of CH_i. */

Step 4. $CH_i \Rightarrow G_s$: $< ID_i, T_s, alloc(. . , ID_j/t_j/\sigma^1_{j\ldots,}), \sigma_i, z_i >$ /* A CH i broadcasts the message allocation. */

Steady-state phase

Step 5. $L_j \rightarrow CH_i$: $< ID_i, ID_j, t_j, C, \sigma_j, z_j >$ /* A leaf node j transmits the sensed data to its CH_i. */

Step 6. $CH_i \rightarrow BS$: $< ID_{bs}, ID_i, T_s, F, \sigma_i, z_i >$ /* A CH_i transmits the aggregated data to the BS. */

Homomorphic Encryption Scheme

1. Represent message m as integer m ϵ [0, M - 1] where M is large integer.
2. Let k be a randomly generated keystream, where k ϵ [0, M - 1]
3. Compute c = Enc(m, k, M) = m + k (mod M)

Decryption:

1. Dec(c, k, M) = c - k (mod M)

VI. CONCLUSION

We first analyzed the data transmission issues and the security issues in CWSNs. Then the absence of the symmetric key management for secure data transmission has been discussed. Then, we accessed two secure and efficient data transmission protocols for CWSNs, they are SET-IBS and SET-IBOOS and the feasibility is also analyzed again the routing mechanism. Finally, the comparison in the calculation and results shows that the proposed protocols have better performance than the existing secure protocols for CWSNs. With respect to both computation and communication costs the system efficiency is moderately good.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, "Wireless Sensor Network Technologies for the Info. Explosion Era", Stud. Comput. Intell. Springer-Verlag, 2010, vol. 278.

[2] Y.Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks", IEEE Commun. Surveys Tuts., vol. 8, no. 2, 2006.

[3] A. A. Abbasi and M. Younis," A survey on clustering algorithms for wireless sensor networks" Comput. Commun vol. 30, no. 14-15, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, application-specific protocol architecture for wireless microsensor networks" IEEE Trans. Wireless commn.

[5] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security". Comput. Sc. - Inf. Secur. Privacy, 2006.

[6] C.-K. Chu, J. K. Liu, J. Zhou et al.,"Practical ID-based encryption for wireless sensor network", in Proc. ACM ASIACCS, 2010.

[7] Chris Karlof , David Wagner., "Secure routing in wireless sensor networks: attacks and countermeasures,"2003Elsevier.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a*et al.*, "SecLEACH-On the security ofclustered sensor networks," *Signal Process.* vol. 87, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of asecure clustering protocol for sensor networks," in *Proc. IEEE NCA*, 2007.

Anil Kumar K received B.E degree in Computer Science Engineering from Ghousia college of engineering and currently doing M.Tech degree in Sapthagiri College of Engineering.

.

Latha.A completed M.Tech and currently working as Assistant Professor in Sapthagiri College of Engineering.

