Abstract:

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. It has been proposed in order to reduce the computation and storage cost to authenticate the encrypted sensed data by applying digital signatures to message packets, which are efficient in communication and applying key management for security. In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based Cryptosystems. Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy. SET-IBOOS is proposed to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management.

Keywords:

WSN, Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission Protocol, ECC.

INTRODUCTION:

Wireless Sensor Networks (WSNs) can provide low cost solutions to various real world problems. WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS,
On the other hand, an attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending bogus information toward the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs. It is because CHs are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes (i.e., CH nodes).

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secure transmission protocols for CWSNs in the literature however, apply the symmetric key management for security, which suffers from the orphan node problem. In this paper, we aim to solve this orphan node problem by using the ID-based cryptosystem that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme [6].

1.RELATED WORK:

The paper[2] author proposed an Adaptive Staggered SLEEP Protocol (ASLEEP) for efficient power management in wireless sensor networks targeted to periodic data acquisition. This protocol dynamically adjusts the sleep schedules of nodes to match the network demands, even in time-varying operating conditions. It uses the CSMA scheme for process the data, but it may be not efficient in fixed WSN network and there is no detail to data management.

The paper[3] author present a cluster based routing algorithm. One of author’s main goals is to design the energy efficient routing protocol. This algorithm makes the best use of node with low number of cluster head know as super node. Here author divided the full region in equal zones and the center area of the region is used to select for super node. Each zone is considered separately and the zone may be or not divided further that’s depending upon the density of nodes in that zone and capability of the super node.

In this paper author considered, cluster head changes when the cluster head is failed. It may be the problem to sensing in that area. The paper [4] author investigate the usefulness of enforcing a minimum separation distance between cluster heads in a cluster based sensor network, thereby prolonging network lifetime by spreading the cluster heads, thus lowering the average communication energy consumption. the minimum separation distance between cluster heads in a cluster based sensor network, thereby prolonging network lifetime by spreading the cluster heads and it shows that our sensor network performs up to 150% better when introducing a minimum separation distance between cluster heads, comparing the number of messages received at the base station, the author consider only about the distance between the cluster heads to improve network lifetime but not energy levels.

2.PROPOSED SCHEME:

When sensor nodes are static in nature, Initially at the time of deployment all node possess unique ID, a certificate (signed by authority i.e. base station), a unique shared key (shared with base station) and a public key of the base station. The certificate is used to authenticate any node at the time of neighbor detection with the public key of the base station; unique shared key is used to communicate with the base station through the lifetime of the network. Network is break by hierarchical approach in to clustered layers. Cluster is a group of nodes with one cluster head (CH). Cluster head responsible for the routing from the cluster to different cluster heads or base station. The process of traveling data is lower clustered layer to higher one. Several techniques are used in current clustering algorithms to achieve longer life time [5]. CH rotation: CH rotation between sensors is necessary because CHs consume more energy than the normal sensors due to their responsibilities of data gathering from sensors and data transmission to the Base Station.

Energy aware CH election: In cluster the node is elected as CH which has high residual energy to even the power usage. Cluster size: Big cluster’s CH consumes more energy than small cluster’s CH. Cluster size is also mattered in energy management. Most popular energy efficient hierarchical clustering protocols are LEACH (Low Energy Adaptive Clustering Hierarchy):it is routing protocol in which the data is delivered to the base station using cluster based approach. In LEACH, cluster heads selected randomly.
The selection of Cluster head depends on decision made 0 and 1. If the number is less than a threshold, the node, becomes a cluster head for the current round. The threshold is set \[ T(n) = \begin{cases} p & \text{if } n \in G \\ 1-p \cdot (r \cdot \text{mod} 1/p) & \text{else} \end{cases} \]

Where \( p \) is the desired percentage of cluster head, \( r \) is the current round. \( G \) is the set of nodes that have not been cluster head in the last \( 1/p \) rounds. This algorithm is simple but does not guarantee about even distribution of cluster heads over the network [19]. In multi cluster security system are using Elliptic Curve Cryptography (ECC) is known to provide equivalent level of security with lower number of bits used. Reduced bit usage implies less power and logic area are required to implement this cryptographic scheme. This is particularly important in wireless networks, where a high level of security is required, but with low power consumption. The equation of an elliptic curve is given as [8],

\[ Y^2 = X^3 + aX + b \]

Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network. The key part of the process is that Alice and Bob exchange their secret key in a mix only. Alice and Bob now use this common secret to encrypt and decrypt their sent and received data. For generation of a shared secret key between A and B using ECDH, both have to agree up on EC domain parameters. Both end have a key pair consisting of a private key (randomly selected integer less than \( n \), where \( n \) is the order of the curve) and another is a public key \( Q = d \cdot G \) (\( G \) is the generator point). Let \((dA, QA)\) be the private-public key pair of \( A \) and \((dB, QB)\) be the private-public key of \( B \).

1. The end A Computes \( KA = (XA, YA) = dA \cdot QB \)
2. The end B Computes \( KB = (XB, YB) = dB \cdot QA \)
3. Since \( dA \cdot QB = dAdB \cdot G = dBdA \cdot G = dB \cdot QA \).
4. Therefore \( KA = KB \) and hence \( XA = XB \)
5. (Where \( G \) is generator point)
6. Hence the shared secret is \( KA \).

Since it is practically impossible to find the private key \( dA \) or \( dB \) from the public key \( KA \)

3. SIMULATION AND RESULTS:

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS-2.34.

![Figure 3.1 Node Verification](image)

In figure 3.1 shows the name output of verification i.e., identifying the authenticated nodes.

<table>
<thead>
<tr>
<th>No of nodes</th>
<th>IBS malicious</th>
<th>IBOOS</th>
<th>Hierarchical Cluster based</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>21.52%</td>
<td>21.25%</td>
<td>47.98%</td>
</tr>
<tr>
<td>100</td>
<td>24.6%</td>
<td>24.8%</td>
<td>55.8%</td>
</tr>
<tr>
<td>200</td>
<td>28.5%</td>
<td>28.4%</td>
<td>65.90%</td>
</tr>
</tbody>
</table>

Table 1: Energy levels for Packet Delivery of hello.

The above table describe the energy level of the packets of hello message for different nodes.

![Figure 3.2 Packet Delivery](image)

In figure 3.2 shows packet delivery. From above figure we can see the Xgraph for the analysis of Energy levels in Cluster IBS mali, Security SET-IBOOS, Hierarchical Cluster based IBOOS. X-axis consists of time in seconds and Y-axis consists of packets.
Fig 5.5: The Energy levels of SET-IBOOS, Hierarchical Cluster based IBOOS From above figure we can see the Xgraph for the analysis of the IBOOS consisting of Energy level 22% and MIBOOS consisting of Energy level is 46%. X-axis consists of time in seconds and Y-axis consists of Energy.

4. CONCLUSIONS:

The Security and Data Transmission in Cluster founded Wireless Sensor Networks. The Offered SET-IBS and SET-IBOOS to protect and effective transmission protocols, respectively for Cluster founded Wireless Sensor systems. SET-IBS and SETIBOOS are produced in connection and applying the ID based crypto-system, which accomplishes security in multi cluster security system, as well as clarified the orphan node difficulty in the protected transmission protocols with the symmetric key management, using SET-IBOOS and SET-IBS are less auxiliary security overhead is preferential for secure data transmission. Future advancement shows the energy consumption for every node in the network with the transfer data in secure and efficient for multi cluster security system.

REFERENCES:

1. “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks” Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE, 2014.
4. Ewa Hansen, Jonas Neander, Mikael Nolin and Mats Björkman “Energy-Efficient Cluster Formation for Large Sensor Networks using a Minimum Separation Distance”,