Secure and Efficient Protocols with Key Management in Dynamic Wireless Sensor Network

Ahmed Abdulhasan Jinah
Student, Department of Computer Science, DR.D.Y Patil College, Pune, India

ABSTRACT: Recently, wireless sensor networks (WSNs) have been established for vast diversity of applications such as military tracking, health care monitoring, traffic monitoring, where sensor nodes are frequently move from different locations. Secure data transmission in wireless sensor network is a challenging task. A good encryption key management protocol is required to secure data and communication. Clustering is a novel approach and practical way out to increase the system performance of WSNs. Proposed system presents an effective key management to secure data transmission for WSNs, in which the clusters are designed. Proposed work present two secure and efficient data transmission protocols for WSNs, called IBS and IBOOS, by using the identity-based digital signature (IBS) technique and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In IBS, network security depends on the use of the Diffie-Hellman problem in the pairing domain. SEDT-IBOOS reduces the computational overhead for protocol security, which is important for WSNs, while its security depends on the wireless network design. Proposed system show the feasibility of the effective key management with SEDT-IBS and SEDT-IBOOS protocols with use of security requirements and security analysis against various attacks such as passive attack, known key attack and impersonation attack. We have discussed a novel integrated approach of IBS and IBOOS for effective key management. We have provided experimental evaluation of the proposed protocol through simulation results.

KEYWORDS: Wireless sensor networks, IBS, IBOOS, keymanagement scheme.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a distributed network of small sensor nodes deployed in large numbers to monitor the environment or other systems by the measurement of physical parameters such as temperature, pressure, or relative humidity. These nodes by monitoring, collects the detailed information about the physical environment in which they are installed, then transmits the collected data to the Base Station (BS). BS is a gateway from sensor networks to the outside world. The BS has a very large storage and large data processing capabilities. It passes the data it receives from sensor nodes to the server from where an end user can access them. The sensors nodes are generally deployed around the area of the BS. A straightforward method to collect the sensed information from the network is to send each sensor node reading to be forwarded to the base station, via other intermediate nodes, before the base station processes the received data. However, this method is expensive in terms of communication overhead, which prompted active research to design an energy-efficient mechanism[1,2]. In fig. 1.1, a generic WSN scenario is shown in which there are seven clusters and sensor nodes are distributed in each cluster. The sensor nodes are sending the sensed data to BS in multi-hop fashion via cluster head to cluster head. In this architecture there are multiple sources and one destination.
A sensor node is made up of four basic components such as sensing unit, processing unit, transceiver unit and a power unit which is shown in fig. 1.2. It also has application dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analogue to digital converters (ADCs)[4]. The analogue signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit is generally associated with a small storage unit and it can manage the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units can be supported by a power scavenging unit such as solar cells. The other subunits of the node are application dependent. This is very common structure of sensor node which is used in WSN.

II. LITERATURE SURVEY

<table>
<thead>
<tr>
<th>Name of the paper</th>
<th>Author name</th>
<th>Proposed scheme and Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1] Effective key management in dynamic wireless sensor network-2015</td>
<td>eung-Hyun Seo, Jongho Won, Salmin Sultana</td>
<td>Proposed a CL-EKM scheme, which also provides forward and backward secrecy.</td>
</tr>
<tr>
<td>3] A key predistribution scheme for sensor networks using deployment knowledge-2014</td>
<td>Pramod K. Varshney</td>
<td>Advantage of the prior knowledge about deployment and reduces the number of unnecessary key spaces carried by each sensor.</td>
</tr>
</tbody>
</table>
III. PROPOSED METHODOLOGY & DISCUSSION

1. Objective of System
The objective of this proposed system is to secure data transmission along with key management.

2. To secure data transmission by using advantage of IBS and IBOOS protocols.

3. To reduce the delay of the system, and to increase the throughput rate by measuring the successful delivered packet through the transmission.

4. To reduce the transmission overhead of shares by using Key management.

5. Robust path finding and path reconstruction.

6. To reduce the energy consumption of the proposed system.
2. Proposed system
The proposed architecture of our system is shown in figure 2.1. Proposed architecture address the problem for security verification with using key management. In this proposed system different key management techniques are used which includes individual key, pairwise key, cluster key, public key private key cryptography for effective and secure key management.
ALGORITHMS

1. **RSA Algorithm**
   RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone.

2. **SHA Algorithm**
   A cryptographic hash is a kind of signature for a text or data file. SHA-256 generates an almost unique 256 bits signature for a text. A hash is not encryption; it cannot be decrypted back to the original text.

3. **ECIES Algorithm**
   Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receivers public key and the receiver will decrypt its private key.

4. **Routing Algorithm**
   For each visited node u, dist[u] is the shortest distance from source to u; and for each unvisited v, dist[v] is the shortest distance via visited nodes only from source to v (if such a path exists, otherwise infinity; note we do not assume dist[v] is the actual shortest distance for un-visited nodes).

IV. EXPERIMENTAL RESULTS

1. **Initialize network**
   The very first step of system, where we have to give the number of nodes in the network, after that select source and destination to send a message. After selecting the source and destination, select the file which we have to send and click on encrypt to encrypt that file. Then click on show network to create a network.

2. **Message encryption**
   After formation of clusters in a network, the CHs broadcast the cluster information which includes the cluster key, information about new node added and node deletion. Then all nodes generate its own private key with help of individual key, which is used to encrypt message. The pairwise key and cluster are also generated while sending message from source to destination. The figure shows message is successfully encrypted.
3. Message sending from source to destination

How packet is send from source to destination with the help of intermediatenodes. Theintermediatenodesarenothingbuttheclusterheadsandthe sensor nodes. The message is Send via shortest path between source and destination.

4. Message decryption

How decryption is done on the destination side. Decryption needs the source’s public key and destination private key. After successful decryption the message is received at the destination.
5. Communication Graph
   The communication graph, as we send a message from one node to other node. The source and destination can be in same cluster or in different clusters. So, the communication graph shows how the data is send from cluster head to cluster head if source and destination are in different clusters.

6. Encryption and decryption timing graph
   The message encryption time, message sending time and message decryption time with respect to number of nodes for 100mb file size.
7. Key generation graph

The key generation time for RSA and ECIES algorithms with different key sizes. The key generation time is calculated in milliseconds with respect to different key sizes of algorithms. From this graph, we can analyze that which algorithm with how much key size is suitable for our system. The graph shows that RSA-512 need less time than RSA-1024 and RSA-2048. And the ECIES-192 is also need very less key generation time. So from this graph we can conclude that, as key generation time is less it will not spend more energy key generation time and help to improve the efficiency of the proposed system.

V. CONCLUSIONS

Through this dissertation, we have addressed effective key management using IBS and IBOOS protocols. IBS and IBOOS protocols are more active than traditional passive techniques.

- We present an algorithm to generate the keys for efficient key management which gives the more security.
to the data sending over the network.

- We have successfully integrate the IBS and IBOOS approach.
- Analysis and experiments show the better results as compared with existing system. The main goal of this research is concerning the protocols IBS and IBOOS have better performance than the existing secure protocols for WSN.

### ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN</td>
<td>Wireless sensor network</td>
</tr>
<tr>
<td>IBS</td>
<td>Identity based digital signature</td>
</tr>
<tr>
<td>IBOOS</td>
<td>Identity based online and offline digital signature</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic curve Cryptography</td>
</tr>
</tbody>
</table>

### REFERENCES