IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Secure Data Transmission with Hierarchical Clustering Based WSN

Shital Mohan Mane[1], Asst Prof. Madhav D. Ingle[2]

Computer Engineering Department, JSCOE, Pune, India[1, 2]

Abstract: A wireless sensor network (WSN) is a network system for geographically distributed resources using wireless sensor nodes to observe physical or environmental conditions such as temperature, motion, and sound. The nodes are individually capable to send data to one or more collection points in a WSN to sense their environments and processing the information data locally. WSNs are great solutions for most applications and security is often a major concern. Though research regarding cryptography, secures routing, key management, intrusion detection, and secure data aggregation in WSNs is done until today, there are still some challenges to be addressed. These challenges are like first selection of proper cryptographic method second factors affecting sensors like memory, speed, and bandwidth, third challenge is, most of the available protocols assume that the sensor nodes and the base station are stationary. Sensor node and base stations in some situations like battlefield need to be mobile. The sensor network topology is been extensively affected by mobility of sensor nodes and so raises many issues about secure routing protocols. This paper surveys various security issues related to cluster based WSNs and existing security protocols.

Keywords: Cluster-based WSNs, ID based digital signature, Secure data transmission, wireless sensor networks, secure routing protocol.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) indicates massive improvement on traditional wired sensor networks. WSNs can greatly simplify system operation and design, as the environment being observed does not need the energy or communication infrastructure associated with wired networks [1]. WSNs are solving many applications like tracking and detecting the passage of tanks and troops on a battlefield, observing environmental pollutants, tracking the location of personnel in a building, and measuring traffic flows on roads. Mostly sensor networks posse's mission-critical tasks [2, 3] so security needs to consider. Using forged information or improper use of information results in unwanted information leakage and inaccurate results. As WSNs used more frequently and grow rapidly, the need for security in them becomes more obvious. However, the behavior of nodes in WSNs gives rise to limitations such as limited energy, processing capability, and storage capacity. These limitations make WSNs very distinct from traditional ad hoc wireless networks. As such, special techniques and protocols have discovered for use in WSNs.

A. Structure of WSNs

A WSN is generally collection of hundreds or thousands of sensor nodes. These sensor nodes are heavily arranged in a sensor field and have the ability to gather data and route data back to a base station (BS). A sensor has four basic parts: a processing unit, a transceiver unit, a power unit and a sensing unit [4]. It may also have extra application- dependent parts such as a power generator, mobilize, and location finding system. Sensing units is a collection of two subunits: analog-to-digital converters (ADCs) and sensors. The ADCs transfer the analog signals generated by the sensors to digital signals based on the observed circumstance. The processing unit, which is usually collide with a small storage unit, arrange the procedures that make the sensor node interact with the other nodes. A transceiver unit links the node to the network. One of the major units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells). Most of the sensor network sensing tasks and routing techniques require knowledge of location, which is been given by a location finding system. Lastly, a mobilize may sometimes be needed to move the sensor node, depending on the application. The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [4]:

II. RELATED WORK

Wireless sensor networks are great solution for this communicated world by internet. Due to WSNs, it is possible that all the remote applications could come in our range [1, 3,4].However, this technology from its invention is still not overcome the issue of security which is challenge for researchers yet [2]. Although there are security protocols available to limit data, leakage there is still need to find proper solution. There are some existing protocols are mentioned in this survey as below.

1. LEACH Protocol[5]:

In 2002, research [5] proposed an application specific protocol for wireless micro sensor network. In this research author developed and analyzed low-energy adaptive clustering hierarchy (LEACH), a protocol

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

architecture for microsensor networks that collects the concept of media access and energy-efficient cluster-based routing application-perceived quality and lifetime. In this method LEACH algorithm adopt clusters and rotate cluster head to evenly distribute load among nodes.
Constraints that limit applicability of LEACH are: In LEACH there is not efficient use of a bandwidth when not all nodes are been connected to cluster head due to sensors always transmit data to the cluster head during their allocated TDMA slot. Second, current design of a LEACH is not suitable for wider range of a micro sensor networks which limits scalability because here author assumed that all nodes are within communication range of each other and the base station. Third, using fixed clusters and rotating cluster head nodes within the cluster may require more transmit power from the nodes. Fourth here author showed that using data aggregation reduces energy dissipation and latency in data transfer compared with an approach like MTE that cannot take advantage of local data correlation.

2. Identity Based Security for Vehicular Ad-HOC Networks.[6]
Jinyuan Sun,et al. in 2010 [6] proposed a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, nonrepudiation, message integrity, and confidentiality. Author contributed privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication.
Author contributions are This is a pseudonym-based scheme to assure vehicle user privacy and traceability. Second, this design is a threshold signature-based scheme to achieve non frame ability in tracing law violators. In this scheme, an innocent vehicle could not framed by a corrupted law enforcement authority due to this role-splitting mechanism. Third, A novel privacy-preserving defense scheme is proposed leveraging threshold authentication. It guarantees that any additional authentication beyond the threshold will result in the revocation of the misbehaving users. Fourth, this scheme incorporates mechanisms that guarantee authentication, no repudiation, message integrity, and confidentiality.

3. Authentication Framework Based On Identity Based Signature For WSNs.[7]
To address the problem of authentication in WSNs, author proposed an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user. The proposed framework is been also evaluated using the most efficient and secure identity-based signature schemes. Existing broadcast authentication schemes in WSNs do not handle the problem of authenticated broadcast by sensor nodes proposed framework is efficient solution to this problem.
In future there is improvement to focus on user access control to provide a complete ID-based authentication to control user access according to his access privilege. In future proposed framework will upgrade on real sensor nodes to get actual results.

4. Secure Routing Protocol for Cluster-Based Wireless Networks [8].
In this approach, author introduced a novel secure routing protocol for cluster-based WSNs using ID-based digital signature. The proposed protocol is efficient in communication, and it achieves all the requirements in security for routing protocols in cluster-based WSNs. This scheme is been pointing the deficiency of the secure routing protocols with symmetric key pairing. However, the simulation results point out the issues in the proposed protocol that, the extra energy consumption by computation of the auxiliary security overhead is still large in the proposed protocol. The future work is to improve our simulation experiments with other secure routing protocols for better results, and improve the protocol in energy efficiency with pairing.

III. PROPOSED SYSTEM

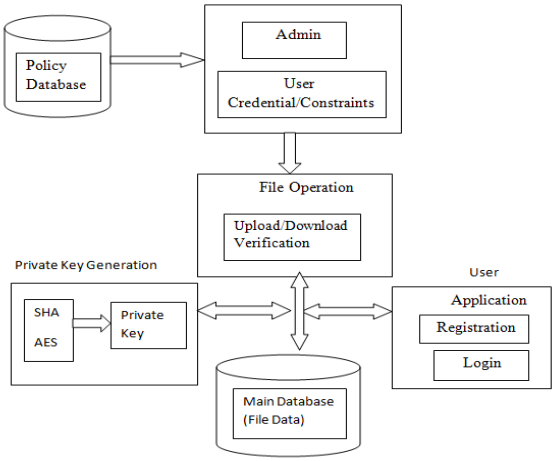


Fig 3.1: Proposed System

In this system we are going to design two secure protocols SET-IBS and SET-IBOOS to manage security in wireless sensor networks. We propose two novel SET protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme, respectively
A cluster based wireless sensor network (WSN) is a network system for geographically distributed resources using wireless sensor nodes to observe physical or environmental conditions, such as temperature, motion, and sound. WSNs are great solutions for most applications and security is often a major concern.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Phases of system

1. System Initialization:
In our scheme, the base station plays the role of PKG, a trustworthy entity, and initializes the system in this phase. Let SKBS be the secret key of the base station. The base station computes the corresponding public key PKBS and sets up the public system parameters SP which include PKBS. The master secret key SKBS is only kept by the base station while SP is made public.

2. Key Generations:
In this phase, the base station computes the secret keys of all sensor nodes corresponding to their IDs using the master secret key SKBS. For a sensor node i with identity IDi, the corresponding secret key is IDi computed as IDi KE(IDi;SKBS). IDs, corresponding private keys and system parameters are stored on sensor nodes before deployment. Hence, every sensor node i stores $\{ID_i;D_{IDi}$, SP}.

3. Message Broadcast and Authentication:
In this phase, the sensor nodes broadcast authenticated messages which are verified using their IDs. The signature generation of a broadcast message is divided into two phases:

Offline phase: The offline phase is performed by the base station, before the message to broadcast becomes available.

Online phase: Whenever a sensor node i senses an event which requires quick reporting, the online phase starts. In this phase, the sensor node i retrieves the partial signature S calculated during the offline phase.

Authentication: On receiving a broadcast message, receiver first checks the time stamp TS to avoid the verification of a replayed message. If it is a fresh one, the receiver further proceeds with signature verification; otherwise it discards the message.

4. Sender Revocations:
To revoke a compromised sensor node i, the base station broadcasts its identity IDi to all other sensor nodes in the network, who store IDi. If in the future a sensor node receives a message containing IDi, it simply rejects the message without going through authentication process. An adversary is assumed to compromise only a few sensor nodes in the network. If the adversary compromises majority of the sensor nodes, it will break down all the security mechanisms. Therefore, storing the IDs of few compromised nodes would incur a reasonable storage overhead for sensor nodes.

IV. MATHEMATICAL MODEL

S: system
1. Login L→S
2. Member registration M→RT
3. Initialization of Protocols SET-IBS and SET-IBOOS.
   - Extraction:
     - First generate private key generated from master key and id of node.
     - Pk= (mk, IDn).
   - Sigining:
     - Generate offline and online signature based on encrypted data.
     - H= (En, IDn)
     - Signature sent in form of (En, IDn, SIG_{online}).
   - Verification: check whether message is authentic or not.

$$SIG_{online} = \text{valid}$$

A. SET-IBS Protocol
The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes:

- **Setup:** The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
- **Extraction:** Given an ID string, a sensor node generates a private key PKID associated with the ID using mk.
- **Signature signing:** Given a message M, time stamp t and a signing key, the sending node generates a signature SIG.
- **Verification:** Given the ID, M, and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

B. SET-IBOOS Protocol
An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes:

- **Setup:** Same as that in the IBS scheme.
- **Extraction:** Same as that in the IBS scheme.
- **Offline signing:** Given public parameters and time stamp t, the CH sensor node generates an offline signature SIGoffline, and transmit it to the leaf nodes in its cluster.
- **Online signing:** From the private key sekID, SIGoffline and message M, a sending node (leaf node) generates an online signature SIGonline.
- **Verification:** Given ID, M, and SIGonline, the receiving node (CH node) outputs "accept" if SIGonline is valid, and outputs "reject" otherwise.

C. AES pseudo code:
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])

DOI 10.17148/IJARCCE.2016.56139

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

```
Begin
byte state[16];
state = in;
AddRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for SubBytes(state);
ShiftRows(state);
AddRoundKey(state, round_key[Nr]);
End.
```

V. EXPECTED RESULT

SET-IBS and SET-IBOOS, in addition with this we presents effective key based schemes to achieve immediate broadcast message authentication.

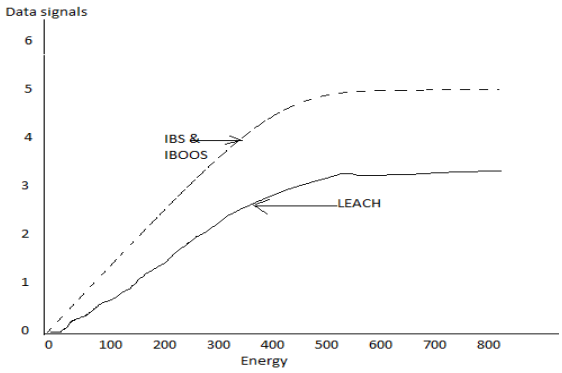
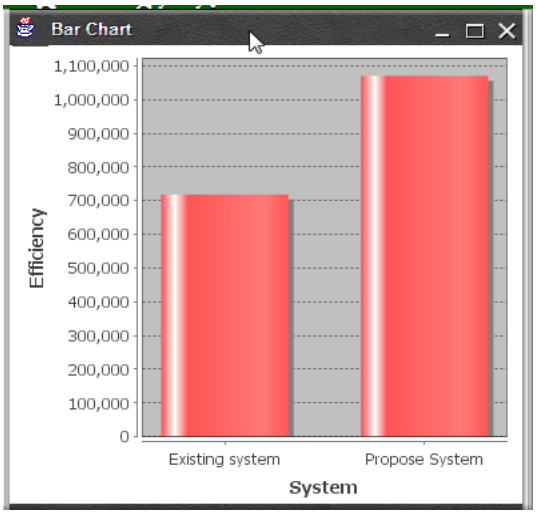


Fig: Energy Efficiency



VI. CONCLUSION

According to authors, contributions this survey predicts that SET_IBS and SET_IBOOS are the efficient protocols until now for cluster based wireless networks to fulfil security requirements we can adopt this protocols in our design to fulfill goals of security in cluster based wireless sensor networks.

VII. FUTURE WORK

To increase network lifetime and to reduce the power consumption of nodes, clustering of nodes is formed. To prevent a system against robust attacks and efficient for large WSNs K-medoid protocol is used for clustering.

REFERENCES

[1] Huang Lu, "Secure and efficient data transmission Cluster-Based wireless Sensor Network "Jie Li Senior Member IEEE Transaction on Parallel and distributed System, March 2014.
[2] D. Estrin et al., "Instrumenting the World with Wireless Sensor Networks," Proc. Int'l. Conf. Acoustics, Speech and Signal Processing, Salt Lake City, UT, May 2001.
[3] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", IEEE Comp. Mag., Oct. 2003, pp. 103–05.
[4] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.
[5] I. F. Akyildiz et al., "A Survey on Sensor Setworks," IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.
[6] Wendi B. Heinzelman, Anantha P. Chandrakasan , Hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Transactions On Wireless Communications, Vol. 1, No. 4, October 2002, pp. 660-670.
[7] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 21, No. 9, September 2010, pp. 1227-1239.
[8] Rehana Yasmin, Eike Ritter, Guilin Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures", IEEE International Conference on Computer and Information Technology, 2010, pp. 882-889.
[9] Huang Lu, Jie Li, and Hisao Kameda, "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature", IEEE Globecom 2010 proceedings, pp.1-4.
[10] Huang Lu, Jie Li, Mohsen Guizani, " Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 3, March 2014, pp. 750 761