Secure and Efficient Data Transmission in Cluster-Based Wireless Sensor Networks Using SET-IBS and SET-IBOOS Protocols for Healthcare Monitoring and Biomedical IoT Systems

Dr. Hana Kim[1]
Prof. Giulia Conti[1]
[1] University of Toronto, Department of Biomedical Cybersecurity and Wireless Sensor Networks, Toronto, Canada

ABSTRACT

Secure data transmission is a critical issue for wireless sensor networks. Clustering is an effective and practical way to enhance the system performance of wireless sensor networks. Study a secure data transmission for cluster-based wireless sensor networks, where the clusters are formed dynamically and periodically. To propose two Secure and Efficient data Transmission (SET) protocols for cluster based wireless sensor networks, 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. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for wireless sensor networks, while its security relies on the hardness of the discrete logarithm problem. Feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for cluster based wireless sensor networks, in terms of security overhead and energy consumption.

KEYWORDS: WSN, Cluster Head(CH), SET-IBS, SET-IBOOS.

1. INTRODUCTION

A WSN is a network where the devices are spatially distributed using wireless sensor nodes. These wireless sensor nodes are used to monitor environmental or physical conditions, such as pressure, motion, sound, temperature etc. These nodes are capable of sensing their environmental conditions, process the information data, and sending data to one or more points in a WSN. The deployment of wireless sensor nodes was motivated by military applications such as battle-surveillance, many industrial and commercial applications. Often the deployment of wireless sensor nodes in adversary, neglected and harsh systems causes a great threat to the society. Transmission of data in secure and efficient manner is one of the most critical issues for WSNs. Secure and efficient data transmission is very much necessary. This has been demanded in many practical WSNs. Network scalability and management maximizes node lifetime and reduces bandwidth consumption by using local collaboration among sensor nodes. In order to achieve this, data transmission based on clusters has been investigated.

Sensor network is divided into number of levels. The sensor nodes from sensor network form the cluster of different size at different levels. Each cluster has a CH. The information sensed by each node is transmitted to CH. Each CH gathers the data from its cluster members, compresses it and sends the compressed data to the base station. Since most of the energy is dissipated during the transmission, the energy optimization technique has been used. The clustering based routing protocol views that each CH within a cluster carries the responsibility of delivering the message to the base station. When there are more number of CHs elected by themselves the overall energy consumed is more. This results in the increase in the overhead of transmission and energy consumption of the system. It requires comparatively high amount of energy for a sensor node to transmit data to the distant CH. Nowadays asymmetric management has been found feasible for WSNs in comparison to symmetric management for security. In asymmetric key management systems digital signature is

one of the most important security services offered by cryptography. There is a bond between the public key and the signer identification. This is obtained via a digital certificate. Recently, the technique of IBS and IBOOS has been developed for secure and efficient transmission of data. As a key management for security, IBS has been developed in WSNs. In order to decrease the storage costs and computation of signature processing the IBOOS scheme has been developed. A general technique for online-offline schemes for signature was introduced. The offline phase executes on a node or at the BS before communication. The online phase executes during communication.

2. PROTOCOLS AND SPECIFICATION

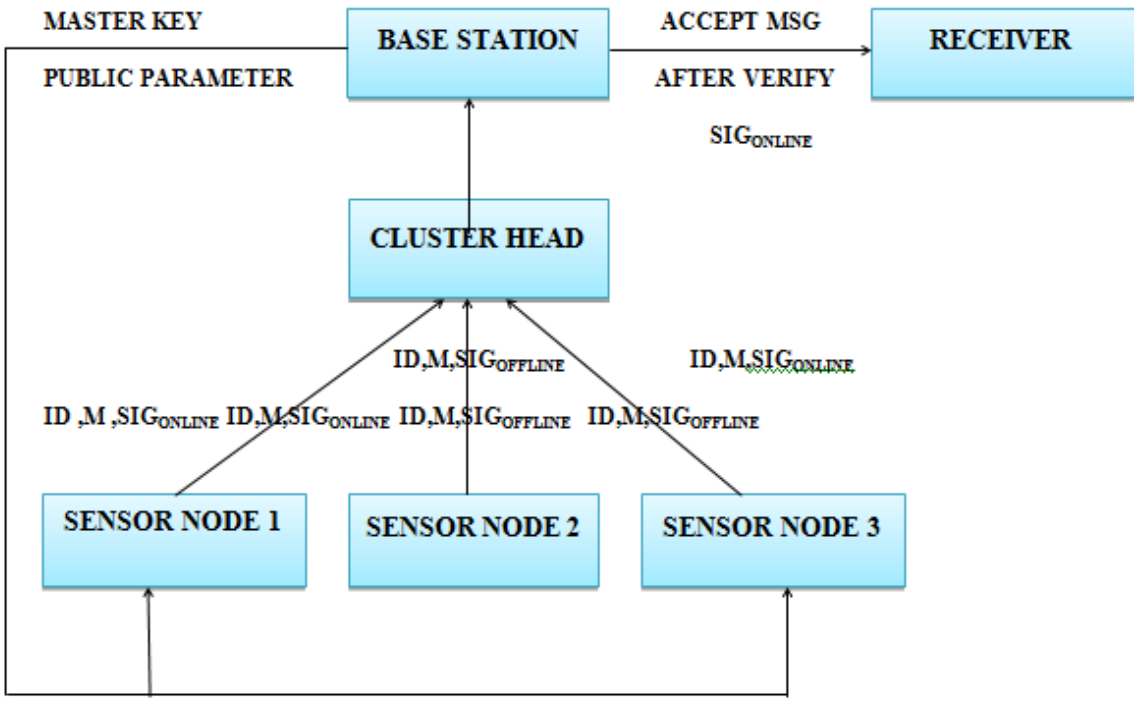
Identity Based digital Signature (IBS): The Identity Based digital Signature is used to compute nodes public key from its unique identity. The IBS scheme performs following four operations: i) Setup: The BS, which acts as a trusted authority generates a master key, MSK, and the public parameters, param, for the private key generator, PKG, and distributes it to all leaf nodes.ii) Extraction: With its own unique ID the sensor nodes generate the private key with the help of MSK provided by the BS. iii) Signature Signing: With the help of message M, time stamp t and signing key, the sending node generates a signature SIG. iv) Verification: Given the message M, ID and the sender node generated signature SIG, the receiver node accepts the message M is the SIG is valid else it is rejected.

Identity Based Online/Offline digital Signature (IBOOS): The Identity Based Online/Offline digital Signature scheme was proposed to reduce the cost for storage of signature processing and reduce the computation. The offline phase can be executed on individual node or at the BS while during communication online phase was used. The offline scheme lacks reusability as it is pre-computed by the third party. The operations performed by the IBOOS scheme are as follows: i) Setup: The BS generates a master key MSK and the public key parameters, param, for the generation of private key at the sender node, and sends it to all the leaf nodes. ii) Extraction: With the help of its unique ID the nodes create a private key with the help of MSK manipulated by the BS. iii) Offline Signing: With the help of public parameters and the time stamp t, an offline signature SIGoff is generated by the CH and it is transmitted to all the leaf nodes in the cluster. iv) Online Signing: With the help of private key, generated by the sensor node with the help of MSK, offline signature SIGoff and message M, a sending node generates an online signature SIG on. v) Verification: Given ID, message M and online signature SIG on, the receiver node validates the message if the online signature is valid else rejected.

Modules Specification

A. Initialization Phase: In this module construct CWSN. In which sensor nodes are grouped into clusters, and each cluster has a cluster head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained.

Figure:



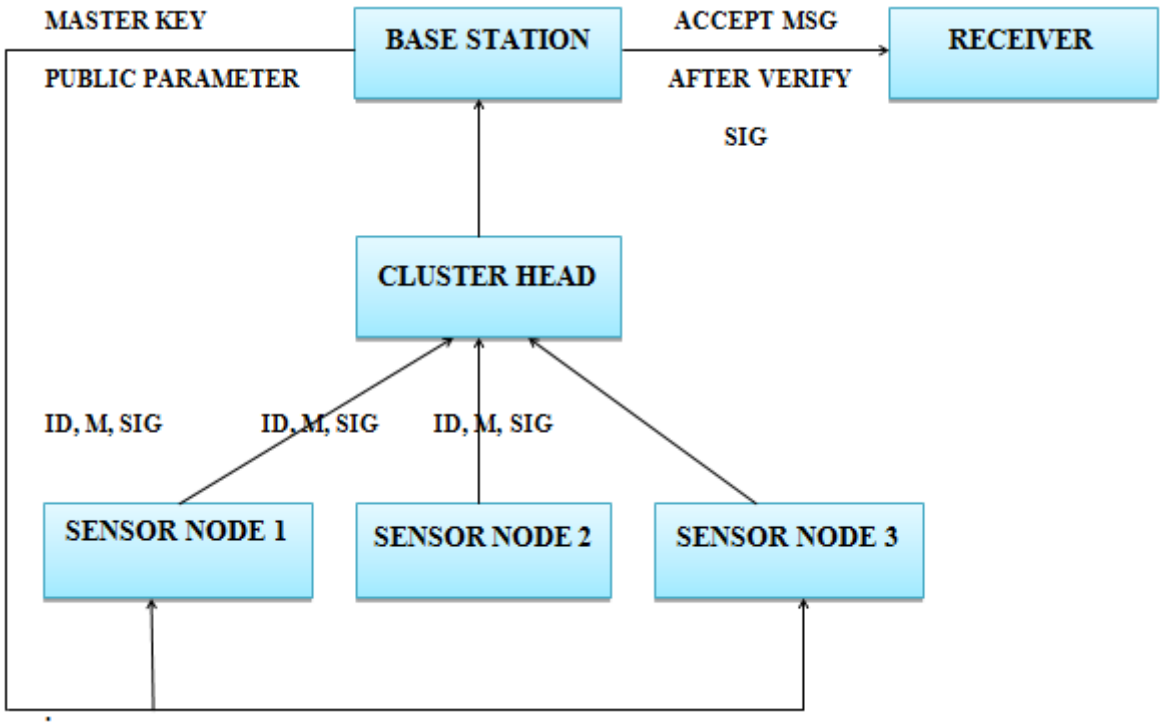
ARCHITECTURE OF SET-IBS

B. Cluster Forming: In this module fixed base station for cluster-base wireless sensor network.Base station responsibility to give authority (certificate and key) for every node incluster,cluster forming that decides which cluster head a sensor should be associated with. The criteria can be described as follows: for a sensor with tentative status or being a cluster member, it would randomly affiliate itself with a cluster head among its candidate peers for load balance purpose. In the rare case that there is no cluster head among the candidate peers of a sensor with tentative status, the sensor would claim itself and its current candidate peers as the cluster heads.

C. SET-IBS: In this module construct SET-IBS which expand as Identity-Based digital Signature (IBS) scheme in this module base station generates a master key and public parameter for private key generator and give that all to sensor node in cluster. Then sensor node generate private key use a private string after that send message along with timestamp and signature. Here signature is generated by signing key. In receiver side message accepted if verification of signature is valid otherwise reject.

D. SET-IBOOS: In this module construct SET-IBOOS which expand as Identity-Based Online/Offline digital Signature (IBOOS) scheme in this module base station generates a master key and public parameter for private key generator and give that all sensor node in cluster. Then sensor node generate private key use a private string after that a cluster head use that sting id and time stamp cluster head generate offline signature send it to the leaf node. And then use the private of sensor node, offline signature and message every sensor node generate online signature .In receiver side cluster head accepted message if signature is online otherwise reject.

Figure:



ARCHITECTURE OF SET-IBOOS

Cluster based Wireless Sensor Network is used to reduce the network consumption and also the increase in energy efficiency. Clustering in WSN is done to minimize the energy consumption and also to reduce the data transmission over the network required to transmit the message to the BS, as the CH becomes responsible for communication, which results into prolonged network lifetime. Initially each node makes decision whether to elect itself as CH for the current round or not. This decision is made on the suggested percentage of CH for the

network and the number of times the node has been elected as CH till now. A node n chooses a random number between 0 and 1. If the random number is less than the threshold Tresh(n), the node becomes CH for the current round. The threshold is calculated using the formulae as shown below: Where p is the desired percentage of CH, r is the current round, G is the set of nodes that have not been CH for the last 1/p rounds. Each node that has elected itself as a CH for current round broadcasts a message as an advertisement to all the other non CH nodes using the same transmission energy. The non CH must keep their receiver open to hear the advertisement from the newly elected CH. The decision to join the CH is done on the advertisement heard with the largest signal strength is the cluster to whom minimum amount of transmission energy is required. If it ties than a random CH is selected. Cluster Set up phase: As the node decides to which CH it wants to join they need to notify the CH that they want to join and this is done using CSMA MAC protocol. Schedule Creation: Once the CH receives the notification from the nodes that they want to join it. The CH creates a TDMA schedule for each node in the cluster so that the nodes within its cluster must transmit the data in the allotted time.

3. SECURITY ANALYSIS AND DISCUSSION

Passive attack on wireless channel: Passive attackers are able to perform eavesdropping at any point of the network, or even the whole communication of the network. Thus, they can undertake traffic analysis or statistical analysis based on the monitored or eavesdropped messages.

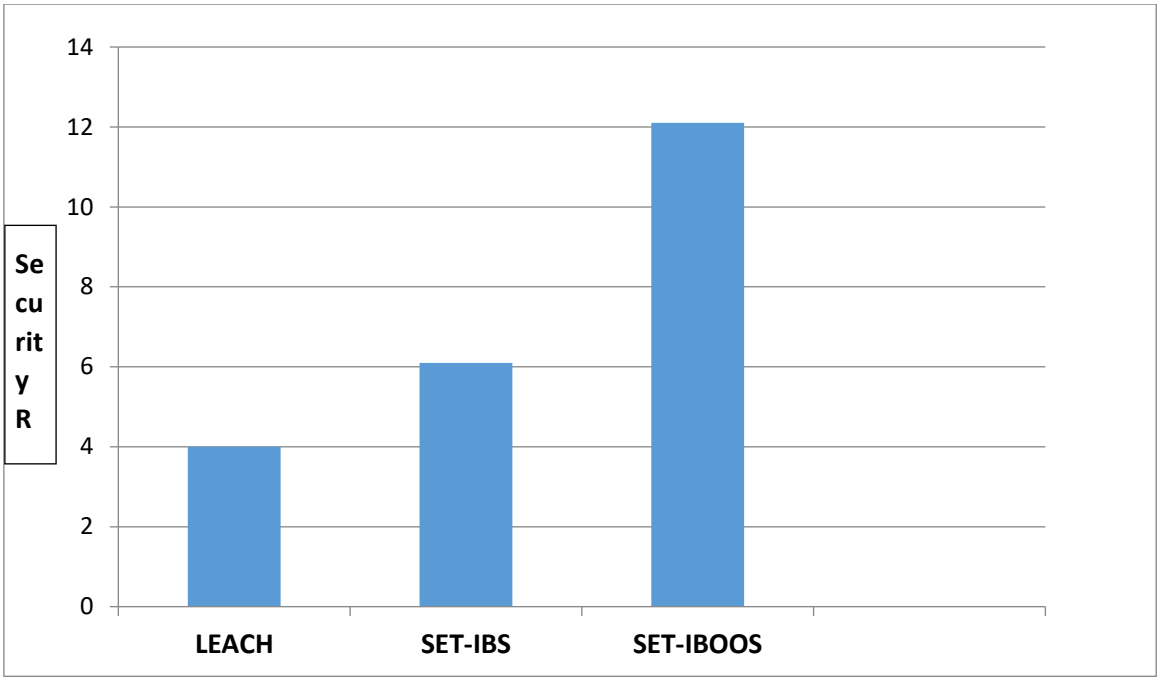
Active attack on wireless channel: Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, the attackers can forge, reply and modify messages. Especially in WSNs, various types of active attacks can be triggered by attackers, such as bogus and replayed routing

information attack, sinkhole and wormhole attack, selective forwarding attack, HELLO flood attack, and Sybil attack.

Node compromising attack: Node compromising Attackers are the most powerful adversaries against the proposed protocols as we considered. The attackers can physically compromise sensor nodes, by which they can access the secret information stored in the compromised nodes, e.g., the security keys. The attackers also can change the innerstate and behavior of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

Symmetric key management was used in LEACH which lead to orphan node problem, occurring because of not sharing the pair wise key with another node in the network, leading to electing itself as a CH which leads to increase in consumption of networks energy. Earlier for secure transmission of data in CWSN asymmetric key management was employed instead of symmetric key, used in LEACH and similar protocols, which uses digital signature. In digital signatures the unique identifier associated with each node is used to create a public key. The main motive of this framework is to provide an authentication framework which solves the problem of energy consumption, storage overhead and the time to process.

Figure:



Comparison of different protocols in Cluster based Wireless Sensor Networks

The results show that the majority of the security is achieved by the SET-IBOOS protocol. Also it depicts an idea of life time of the cluster based Wireless Sensor Networks. The above figure shows that the highest security is achieved by the SET-IBOOS protocol as compared to the other two protocols. By reducing extra computation cost and maximizing more security including time parameter, SET-IBOOS have achieved its excellence in terms of overhead transmission and energy consumption.

4. CONCLUSION

In this paper, it is reviewed that the data transmission issues and the security issues in cluster based wireless networks. The deficiency of the symmetric key management for secure data transmission has been discussed. It is then presented two secure and efficient data transmission protocols respectively for cluster based wireless networks, reliable data transmission identity based digital signature protocol. In the evaluation section, it is provided feasibility of the proposed efficient data transmission identity based digital signature protocol with

respect to the security requirements and analysis against routing attacks. Reliable data transmission identity based digital signature protocol is efficient in communication and applying the ID-based crypto-system, which achieves security requirements in cluster based wireless networks, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.

REFERENCES

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” IEEE Trans. Wireless Commun., vol. 1, no. 4, 2002.
[2] K. Zhang, C. Wang, and C. Wang, “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,” in Proc. WiCOM, 2008
[3] P. Banerjee, D. Jacobson, and S. Lahiri, “Security and performance analysis of a secure clustering protocol for sensor networks,” in Proc. IEEE NCA, 2007.
[4] Huang Lu, Jie Li, Kameda, “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks
[5] Using ID-Based Digital Signature” in H.Global Telecommunications Conference (GLOBECOM 2010), Page(s): 1- 5, Publication Year: 2010.
[6] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” in Lect. Notes. Comput. Sc. - CRYPTO, 2001
[7] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” in Lect. Notes. Comput.Sc. - CRYPTO, 2001.
[8] J. Liu and J. Zhou, “An Efficient Identity-Based Online/Offline Encryption Scheme,” in Lect. Notes. Comput. Sc. - Appl. Crypto. Netw.Secur., 2009

[9] .M. J. Handy, M. Haase, and D. Timmermann, “Low energy adaptive clustering hierarchy with deterministic cluster-head selection,” in Proc. Int. Workshop Mobile Wireless Commun. Netw., Sep. 2002, pp. 368–372.
[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy efficient communication protocol for wireless microsensor networks,” in Proc. 33rd Hawaii Int. Conf. Syst. Sci. (HICSS), Washington, DC, USA, Jan. 2000, pp. 1–10.
[11] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670,Oct. 2002.