Towards Efficient and Secure Transmission of Data for Cluster based Wireless Sensor Networks

Prathima K.M
M.Tech, Dept of Computer Science & Engineering
SJB Institute of Technology
Bangalore-60, India
kmprathima@gmail.com

Manu M N
Asst. Prof, Dept of Computer Science & Engineering
SJB Institute of Technology
Bangalore-60, India
manu2me1@gmail.com

***Abstract*— A Wireless Sensor Network (WSN) is a network formed by large number of sensor nodes where each node is equipped with a sensor to detect physical or environmental phenomena such as light, heat, pressure, temperature, sound, vibration, motion etc. Grouping sensor nodes into clusters has been widely investigated by researchers in order to achieve the network system's scalability and management objectives. Efficient and Secure data transmission is thus necessary and demanded in many applications such as military domain, homeland security, health care, etc. Secure data transmission is a critical issue for wireless sensor networks (WSNs). The two Secure and Efficient data Transmission (SET) protocols such as SET-IBS and SET-IBOOS, by using Identity based Digital Signature and Identity based online/Offline digital signature scheme, respectively are used to provide security and efficient data transmission. These protocols have better performance in term of security overhead and energy consumption. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. SET-IBOOS reduces the computational overhead for security using IBOOS scheme. These two protocols also identify the three kinds of attacks such as active attack, passive attack and node compromising attack.**

Keywords*— Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission protocol.

I. Introduction

A Wireless Sensor Network (WSN) is a network formed by large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure etc. Sensor devices are limited in their energy, computation, and communication capabilities. Sensor networks closely interact with their physical environments and with people, posing new security problems.

Wireless sensor networks have applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. Security in wireless sensor network is different compared to security in LANs, WANs, and Internet etc. This is due to Sensor Node is having Constraints on battery power, CPU and memory and WSN is Wireless, Ad hoc, Unattended. Hence it poses new security problems and research challenges. In WSNs one of the primary security requirements is authentication of entity, message, data, especially in data critical applications.

A. Literature Survey

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. The study of secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically[1]. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge [2].

The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. [4] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. The LEACH can improve system lifetime by an order of magnitude compared with general-purpose multihop approaches [4]. Information retrieval in Wireless Sensor Networks using enhanced APTEEN [5] protocol. The delay in answering the queries depends greatly on the frame length. Frame length can be reduced if all the CHs use different CDMA codes to communicate with the BS.

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links [8]. SecLEACH a protocol for securing LEACH-based networks. Sec- LEACH achieves baseline security by adapting random key predistribution and can yield different performance numbers on efficiency and security depending on its various parameter values.

There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH [8], GS-LEACH [9] and RLEACH [10]. The GS-LEACH protocol is more energy efficient than any of the secure flavors of LEACH. The GS-LEACH (grid-based secure LEACH) protocol uses pre deployment key distribution using prior knowledge of the deployment area. This protocol is very energy efficient and provides a longer network lifetime compared to the other flavors of LEACH [9].

Sensor networks require efficient, low latency key management techniques that enable strong security and tolerance of node compromise by Carman *et al* [15]. Cryptographic community that combines the benefits of both identity-based cryptography and random key predistribution into a framework we call identity-based random-key predistribution (IBRKP).

The secure routing for cluster based sensor networks where clusters are formed dynamically and periodically. The deficiency in the secure routing protocols with symmetric key pairing. Along with the investigation of ID-based cryptography for security in WSNs, a new secure routing protocol with ID-based signature scheme for cluster-based WSNs, in which the security relies on the hardness of the Diffie-Hellman problem in the random oracle model [17]. Novel secure routing protocol for cluster-based WSNs using ID-based digital signature.

A new type of signature scheme is On-Line/Off-Line Digital Signatures was introduced by Even et al [18]. It consists of two phases. The first phase is performed off-line, before the message to be signed is even known. The second phase is performed on-line, once the message to be signed is known, and is supposed to be very fast. The method uses one-time signature schemes, which are very fast, for the on-line signing. An ordinary signature scheme is used for the off-line stage. A variant of Rabin's signature scheme (based on factoring) and DES is used. The IBOOS scheme could be effective for the key management in WSNs. This scheme has been proposed in order to reduce the computation and storage costs of signature processing. The offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

B. *Contribution and Organization*

In this paper, we extend our previous work and focus on providing efficient secure data communication for CWSNs. The contributions of this work are as follows.

- Two **S**ecure and **E**fficient data **T**ransmission (SET) protocols for CWSNs, called **SET-IBS** and **SETIBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.
- Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information.
- SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme. Both SET-IBS and SETIBOOS solve the orphan node problem in the secure data transmission with a symmetric key management.

II. PROPOSED ARCHITECTURE

Consider a CWSN consisting of a fixed base station (BS) and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume that the BS is always reliable, i.e., the BS is a trusted authority (TA). Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, 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.

In CWSNs, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node (e.g., a CH) aggregates data and sends it to the BS is preferred, than the method that each sensor node directly sends data to the BS [1, 3]. A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the TDMA (time division multiple access) control used for data transmission. In this paper, the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWSNs above.

A. *Protocol Objective*

The goal of the proposed secure data transmission for CWSNs is to guarantee a 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 [8–10], however, apply the symmetric key management for security, which suffers from the orphan node problem that is introduced in Section 1. In this paper, we aim to solve this orphan node problem by using the ID-based crypto-system that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

III. NETWORK DESIGN

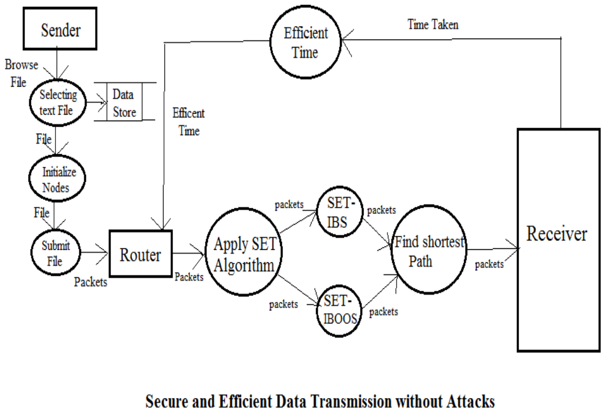


Fig. 1: DFD for Efficient and Secure data transmission without attack

Fig. 1 and 2 shows the dataflow diagram for efficient and secure transmission of data for cluster based wireless sensor networks without and with attacks. The data flow diagram in the Fig. 1 shows how the sender sends the information to the receiver. First the sender selects the text file, this text file is stored. Then by collecting destination IP address and router IP address initialize the nodes. In the initialization process, the base station will generate the secrete key and distribute this key with all the sensor nodes in the network. Then submit file to the router. The router first applies the SET algorithm such a SET-IBS and SET-IBOOS to provide security and efficient data transmission. Later apply the Dynamic Source Routing Protocol to find shortest path to destination. The nodes and attackers status are updated in the router. If the path is found and there is no attack then the data will be delivered to respective node securely and efficiently. Once the data reaches to destination then the router will calculate the efficient time.

The data flow diagram in the Fig. 2 shows how senders data losses during attack. If the router founds the shortest path and also an attack such as active attack, passive attack or node compromising attack then the attack details are showed in router. The data will lost and resend back to the sender by the router.

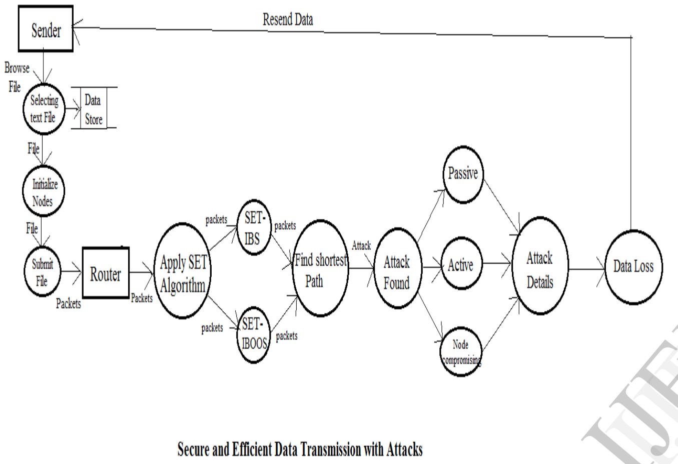


Fig. 2: DFD for Efficient and Secure data transmission with error

IV. IBS AND IBOOS FOR CWSN

In this section, we introduce the IBS scheme and IBOOS scheme used in the paper. Note that the conventional schemes are not specifically designed for CWSNs. We adapt the conventional IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes. In order to further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs.

A. *SET-IBS Protocol*

This protocol is used for secure communication of data. SET-IBS solve the orphan node problem in the secure data transmission with a symmetric key management. The 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 of the data sending nodes, and verification of the data receiving nodes.

1) Protocol Initialization:

a) Setup: The BS (as a trust authority) generates a master key and public parameters for the private key generator, and gives them to all sensor nodes.

2) Key management for Security:

a) Extraction: Given an ID string, a sensor node generates a private key associated with the ID using master key

b) Signature signing: Given a message M, time-stamp t and a signing key θ, the sending node generates a signature SIG.

c) Verification: Given the ID, M and SIG, the receiving node outputs “accept” if SIG is valid, and outputs “reject” otherwise.

3) Protocol Operation:

After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase.

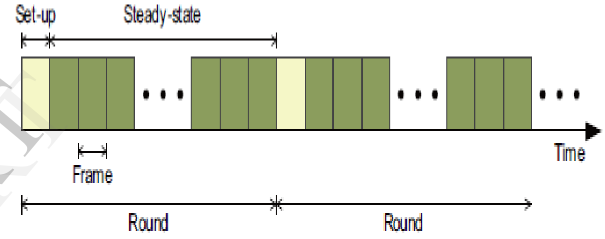


Fig. 3: Operation in the secure data transmission

The operation of SET-IBS is divided by rounds as shown in Figure. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS.

B. *SET-IBOOS Protocol*

This protocol is used for efficient data transmission. This 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 of the data sending nodes, and verification of the receiving nodes.

1) Protocol Initialization:

a) Setup: Same as that in the IBS scheme.

2) Key management for Security:

a) Extraction: Same as that in the IBS scheme.

b) Offline signing: Given public parameters and time-stamp t, the CH sensor node generates an offline signature $SIG_{offline}$, and transmits it to the leaf nodes in its cluster.

c) Online signing: From the private key, $SIG_{offline}$ and message M, a sending node (leaf node) generates an online signature SIG_{online}.

d) Verification: Given ID, M and SIG_{online}, the receiving node (CH node) outputs “accept” if SIG_{online} is valid, and outputs “reject” otherwise.

3) *Protocol Operation:*

The SET-IBOOS operates similarly to that of SET-IBS.SET-IBOOS works in round during communication.

V. Protocol Characteristics

In this part, we summarize the characteristics of the proposed SET-IBS and SET-IBOOS protocols. Table 1 shows a general summary of comparison of the characteristics of SET-IBS and SET-IBOOS with prior ones, in which metrics are used to evaluate whether a security protocol is appropriate for CWSNs. We explain each metric as follows.

a) Key management: The key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

b) Neighborhood authentication: used for secure access and data transmission to nearby sensor nodes, by authenticating with each other.

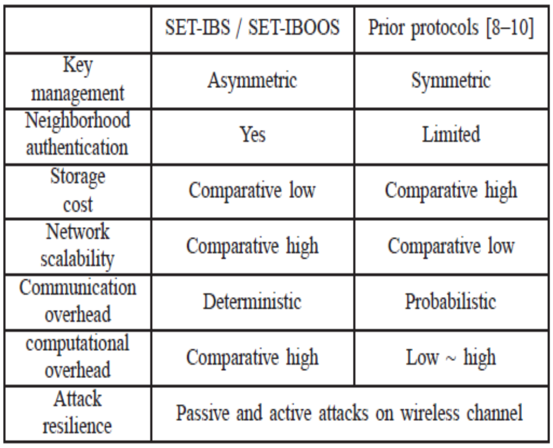
c) Storage cost: represents the requirement of the security keys stored in sensor node's memory.

d) Network scalability: indicates whether a security protocol is able to scale without compromising the security requirements.

e) Communication overhead: the security overhead in the data packets during communication.

f) Computational overhead: the energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.

g) Attack resilience: the types of attacks that security protocol can protect against.



	SET-IBS / SET-IBOOS	Prior protocols [8–10]
Key management	Asymmetric	Symmetric
Neighborhood authentication	Yes	Limited
Storage cost	Comparative low	Comparative high
Network scalability	Comparative high	Comparative low
Communication overhead	Deterministic	Probabilistic
computational overhead	Comparative high	Low ~ high
Attack resilience	Passive and active attacks on wireless channel	

Table 1: Comparison of characteristics of the protocols with other secure data transmission protocols.

VI. Result

For the performance evaluation, we compare the proposed SET-IBS and SET-IBOOS with LEACH protocol [4] and SecLEACH protocol [8].

The implementation efficiently makes use of the available resources of the system. Compared to SecLEACH and LEACH protocols SET-IBS and SET-IBOOS are more efficiently transmits data to the destination and more security is provided to the encrypted sensed data. This system identifies three kind of attacks such as active, passive and node compromising attacks. These kind of attacks are overcome by using SET-IBS and SET-IBOOS protocols. If attacks are occurred in the nodes then the data is not send to destination, will resend back to sender. All error conditions should be handled properly.

Conclusion

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. Then presented different kind os attacks on WSNs. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs.

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. 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, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, 2002.

[5] Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol," IEEE Trans. Parallel Distrib. Syst., vol. 13, 2002.

[6] S. Yi, J. Heo, Y. Cho et al., "PEACH: Power-efficient and adaptive clustering hierarchy protocol for WSNs," Comput. Commun., vol. 30, no. 14-15, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int. J. Comput. Applications, vol. 47, no. 11, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered 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.

[10] 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.

[11] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in Proc. ICCCS, 2011.

[12] G. Gaubatz, J. P. Kaps, E. Ozturk et al., "State of the Art in Ultra-Low Power Public Key Cryptography for WSNs," in Proc. IEEE PerCom Workshops, 2005.

[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," inLect. Notes. Comput. Sc. - CRYPTO, 2001.

[14] Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in Lect. Notes. Comput. Sc. - CRYPTO, 1985.

[15] D. W. Carman, “New Directions in Sensor Network Key Management,” Int. J. Distrib. Sens. Netw., vol. 1, 2005.

[16] R. Yasmin, E. Ritter, and G. Wang, “An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures,” in Proc. IEEE CIT, 2010.

[17] H. Lu, J. Li, and H. Kameda, “A Secure Routing Protocol for Cluster-Based WSNs Using ID-Based Digital Signature,” in Proc. IEEE GLOBECOM, 2010.

[18] S. Even, O. Goldreich, and S. Micali, “On-Line/Off-Line Digital Signatures,” in Lect. Notes. Comput. Sc. - CRYPTO, 1990.

[19] S. Xu, Y. Mu, and W. Susilo, “Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security,” in Lect. Notes. Comput. Sc. - Inf. Secur. Privacy, 2006.

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