ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

The Feasibility of SET-IBS and SET-IBOOS Protocols in Cluster-Based Wireless Sensor Network

R.Anbarasi[1], S.Gunasekaran[2]

P.G. Student, Department of Computer Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India[1]

Associate Professor, Department of Computer Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India[2]

ABSTRACT: A wireless sensor network is a special kind of Ad-hoc network, consist of thousands of small devices which are called as sensor nodes used to monitor physical or environmental conditions Clustering is a critical task in Wireless Sensor Networks for energy efficiency and network stability. In the existing method, a secure data transmission for cluster-based WSNs is presented in which the clusters are formed in a dynamic and periodic manner. A two secure and efficient data transmission protocols for CWSNs is presented which is 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. But the drawback in the existing method is there may lead to leakage of user's public key and secret key in the case of compromised users in the SET-IBS protocol and SET-IBOOS protocol is only efficient for the devices with high computational power. So, in order to overcome this problem an innovative technique is introduced which is called Enhanced Secure Data Transmission protocol which is used to improve the SET-IBS and SET-IBOOS protocol. In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity. Also, to confuse the attackers, encapsulation algorithm is used. In this process, the two cipher texts are used: one is valid cipher text and another one is invalid cipher text. These cipher texts are encapsulated with the corresponding author's encapsulated key. In order to improve the efficiency in the SET-IBOOS protocol, the improved SET-IBOOS protocol is proposed in which the online/offline attribute based encryption method is used. An experimental result shows that proposed method achieves high efficiency and high security.

KEYWORDS: cluster-based WSN's, ID based digital signature, ID-online/offline digital signature, enhanced secure data transmission protocol

I.INTRODUCTION

A wireless sensor network is a group of specialized transducers with a communication infrastructure that uses radio to monitor and record physical or environmental condition and also used in the variety of application such as military sensing and tracking, environmental monitoring, disaster management etc. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN. Secure data transmission is one of the most important issues for WSNs. At the same time, many WSNs are deployed in rough, disregarded, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings. Secure data transmission is especially necessary and is demanded in many such practical WSNs. their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed. To refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

II.EXISTING WORK

Aggregation of same objects or sensors in our context is known as clustering. In cluster-based WSN, all sensor nodes are clustered and a cluster head is elected to manage the operation of its own cluster. Cluster head should aggregate data from all sensor nodes sensed from a specified target. Therefore, CWSN efficiently reduce the amount of information in the entire network Cluster-based data transmission in WSNs has been analyze by researchers to attain the network scalability and management, by using this we can maximizes node period of time and reduce bandwidth consumption by using local collaboration among sensor nodes.

In the existing system, a secure data communication for CWSNs is presented. The contributions of this work are as follows:

- In cluster-based wireless sensor network two secure and efficient data transmission protocols are present called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme, respectively. The key idea behind the SET-IBS and SET-IBOOS protocol is to authenticate the encrypted sensed data, by applying digital signatures In the previous existing 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 depend 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 energy can be saved..
- SET-IBOOS is further used to reduce the computational overhead for security using the IBOOS scheme, in which security depends 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.

Drawbacks:

- Lead to leakage of user’s public key and secret key in the case of compromised users in the SET-IBS protocol
- SET-IBOOS protocol is only efficient for the devices with high computational power
- Less efficient

RREP. Optimization function uses the individual node’s battery energy; if node is having low energy level then optimization function will not use that node.

III.PROPOSED SYSTEM

In the proposed system, an innovative technique in introduced which is called Enhanced Secure Data Transmission protocol (ESDT) which is used to improve the SET-IBS and SET-IBOOS protocol.

- In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity. Also, to confuse the attackers, encapsulation algorithm is used. In the method, by using the corresponding sender’s ID, the message will be encrypted which generates the correct cipher text and wrong cipher text. After that, the correct cipher text and wrong cipher text will be encapsulated with the corresponding author’s encapsulated key and send to the receiver. In the decapsulation process, receivers it will check whether an encapsulated key is match with the original encapsulated key and retrieve the valid message.
- In order to improve the efficiency in the SET-IBOOS protocol, the improved SET-IBOOS protocol is proposed which the online/offline attribute based encryption method is used.

In this initialization stage, the security parameter will be created randomly by using which the public and secret keys are generated. After that the secret identity will be created based on the secret key of sender and identity of cipher text. In the offline encryption, the public parameter will be taken as input to create the first level cipher text. In the online encryption, the first level cipher text, public parameters and attribute values will be taken as input. It will produce session key and cipher text as output. For the decryption, session key and the private key will be used by the receiver to decrypt the given cipher text.

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between leaf nodes and CHs, as well as transmission between CHs and the BS. Also, the computational complexity is an important concern. So, reducing computational complexity with enhancing security in the wireless sensor network is also important concern.

IV.SYSTEM MODULES

ESDT model is used to enhance the security in CWSN’s. The system is divided into four major modules:

1. Initialization of SET-IBS protocol.
2. Operation of SET-IBS protocol.
3. Initialization of SET-IBOOS protocol.
4. Operation of SET-IBOOS protocol.
5. Enhanced Secure Data Transmission

.

1. Initialization of SET-IBS protocol.

Setup phase: In the protocol initialization the Base Station generates a master key *msk* and public parameter *param* for the generation of private key and sends them all to the sensor nodes.

Extraction process: Node j first obtains its private key as from msk and where is its ID$_j$, and is the time stamp of node j's time interval in the current round that is generated by its CH i from the TDMA control.

Signature signing: The sensor node j picks a random number and computes. The sensor node further computes

$c_j = h(C_j \| t_j \| \theta_j).$

$$c_j = h(C_j || t_j || \theta_j$$

$$\sigma_j = c_j sek_j + \alpha_j P,$$

Where $\langle \sigma_j, c_j \rangle$ is the digital signature of node j on the encrypted messageC_j. The broadcast message is now concatenated in the form of $\langle ID_j, t_j, C_j, \sigma_j, c_j \rangle$.

Verification: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the time stamp of current time interval t_j and determines whether the received message is fresh. Then, if the time stamp is correct, the sensor node further computes $\theta_j' = e(\sigma_{j,} P) e(H(ID_j || t_j), -P_{pub})^{c_j}$ using the time stamp of current time interval t_j . For authentication, which is equal to that in the received message, the sensor node considers the received message authentic, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, and ignores it.

2. Operation of SET-IBS protocol.

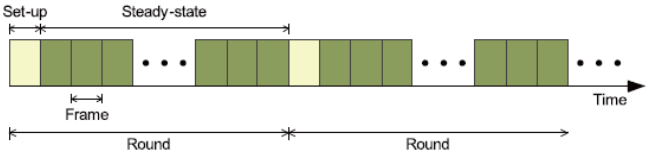

Fig: 1. Operations of protocol.

After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. we suppose that all sensor nodes know the starting and ending time of each round because of the time synchronization. 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. In each round, the timeline is divided into consecutive time slots by the TDMA control. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly elected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. In the setup phase, the time stamp T_s and node IDs are used for the signature generation. Whereas in the steady state phase, the time stamp t_j is used for the signature generation securing the inner cluster communications, and T_s is used for the signature generation securing the CHs to- BS data transmission.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

3.Initialization of SET-IBOOS protocol.

Setup phase: In the protocol initialization the Base Station generates a master key *msk* and public parameter *param* for the generation of private key and sends them all to the sensor nodes.
Extraction process: Before the signature process, node j first extracts the private key from the msk τ and its identity ID, as where

$$R_j = g^{r_j}$$
$$s_j = r_j + H(R_j, ID_j)\tau mod\ q.$$

Offline signing: At the offline stage, node j generates the offline value $< \hat{\sigma}_j >$ with the time stamp of its time slot tj for transmission, and store the knowledge for signing online signature when it sends the message. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, for example, the CH sensor node. Let then

$$g^{s_j} = g^{r_j} g^{H(R_j,ID_j)\tau mod\ q} = R_j X^{H(R_j,ID_j)mod\ q}$$
$$\hat{\sigma}_j = g^{-t_j}$$

Online signing: At this stage, node j computes the online signature based on the encrypted data C_j and the offline signature$\hat{\sigma}_j$.

$$h_j = H(C_j, ID_j)$$
$$z_j = \hat{\sigma}_j + h_j s_j mod\ q$$
$$\sigma_j = g^{\hat{\sigma}_j}$$

Then, node j sends the message to its destination witht_j,R_j and the online signature, in the form of$ID_j, t_j, R, \sigma_j, z_j, c_j$.
Verification process: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the current time stamp t_j or freshness. Then, if the time stamp is correct, the sensor node further computes the values of g^{z_j} and $\sigma_j R_j^{h_j} X^{h_j H(R_j,ID_j)mod\ q,}$. If the values of and $\sigma_j R_j^{h_j} X^{h_j H(R_j,ID_j)mod\ q,}$ are equal from the received message, the node i considers the received message authentic, accepts it, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, then rejects or ignores it.

4. Operation of SET-IBS protocol.

The proposed SET-IBOOS operates same as that of SET-IBS protocol. SET-IBOOS works in rounds during communication, and the self-elected CHs are decided based on their local decisions, thus it functions without data transmission in the CH rotations. However, the differences is that digital signature are changed from ID-based signature to the online signature $\langle \sigma_i, z_i \rangle$ of the IBOOS scheme.

Once the setup phase is over, the system turns into the steady-state phase, in which data are transmitted to the BS.

5. Enhanced secure Data transmission Protocol:

In the proposed system, an innovative technique in introduced which is called Enhanced Secure Data Transmission protocol (ESDT) which is used to improve the SET-IBS and SET-IBOOS protocol. In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity.

IMPROVED SET-IBS PROTOCOL:

. In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity.
Setup phase: The setup algorithm takes as input a security parameter λ and produces the master public key mpk and the master secret key msk. The master public key defines an identity set ID, and an encapsulated-key set K. All other algorithms KeyGen, Encap, Decap, implicitly include mpk as an input.

Key generation: For any identity the KeyGen algorithm uses the master secret key msk to sample an identity secret keysk_{id}.
Valid Encapsulation: The valid encapsulation algorithm creates pairs (C, k) where C is a valid cipher text, and is the encapsulated-key.
Invalid Encapsulation: The alternative invalid encapsulation algorithm samples an invalid cipher text C for a given id.
Decapsulation: The decapsulation algorithm is deterministic, takes a cipher text C and an identity secret key and outputs the encapsulated key k.

IMPROVED SET-IBOOS PROTOCOL:

To improve the efficiency in the SET-IBOOS protocol, the improved SET-IBOOS protocol is proposed which the online/offline attribute based encryption method is used.

Setup phase: The setup algorithm takes as input a security parameter λ and a universe description U, which defines the set of allowed attributes in the system. It outputs the public parameters PK and the master secret key MK.
Extraction process: The extract algorithm takes as input the master secret key MK and an access structure (resp., set of attributes) I_{key} and outputs a private key SK associated with the attributes.
Offline. Encrypt (PK): The offline encryption algorithm takes as input the public parameters PK and outputs an intermediate cipher text IT.
Online. Encrypt (PK, IT,: The online encryption algorithm takes as input the public parameters PK, an intermediate cipher text IT and a set of attributes (resp., access structure) and outputs a session key and a cipher text CT.
Decrypt (SK; CT) → key. The decryption algorithm takes as input a private key SK for I_{key} and a cipher text CT associated with) I_{enc} and decapsulates cipher text CT to recover a session key.

IV.CONCLUSION

Successful data transmission and security can be achieved by using CWSN's. The inadequacy symmetric key management for secure data transmission has been addressed. In previous method, the CWNS's consist of two efficient protocol called SET-IBS and SET-IBOOS protocol. By using SET-IBS and SET-IBOOS provide secure data transmission for CWSN's with concrete ID-based settings, which use ID information and digital signature for authentication.. Thus, both SET-IBS and SET-IBOOS fully solve the orphan node problem from using the symmetric key management for CWSN's. but the disadvantage of this method there is a chance for the leakage of user's public key and secret key in the case of compromised users. So, in the proposed method an enhanced secure data transmission protocol (ESDT) this is used to enhance the security. In this method the valid and invalid cipher texts are created for confusing the attackers. Finally, the comparison in the calculation and simulation results shows that the proposed enhanced secure data transmission protocols obtain more performance and security than the existing secure protocols for CWSN's.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
[2] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.
[3] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
[4] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.
[5] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.
[6] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.
[7] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.
[8] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
[9] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
[10] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.