International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Ensuring Efficient Data Transmission in Wireless Sensor Networks in Secure Way

D. Hemalatha[1], R. Arunudaya[2]

[1, 2]Vel Tech Multi Tech College, Avadi

Abstract: ***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. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, 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 WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the 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 CWSNs, in terms of security overhead and energy consumption.***

Keywords: Wireless Sensor Networks, Secure and Efficient data Transmission protocols, Identity-Based digital Signature (IBS), Identity-Based Online/Offline digital Signature (IBOOS).

1. Existing System

In this Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. 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.

Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

Disadvantages of Existing System

- The clusters are formed dynamically and periodically.
- Existing solutions are provided for distributed WSNs, but not for CWSNs.
- It reduces the possibility of a node joining with a CH.
- Problem occurs when a node does not share a pair wise key with others in its preloaded key ring.

2. Proposed System

In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, 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.

It has been proposed in order to reduce the computation and storage costs 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.

In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

Advantages of Proposed System

- Overcomes the key escrow problem described in ID-based cryptosystems.
- Efficient in communication and saves energy.
- Solve the orphan node problem in the secure data transmission with a symmetric key management.
- More feasibile.

3. List of Modules

1) User Interface
2) Transferring Messages
3) Static and Dynamic Approach
4) Key generation and receiving messages

1. User Interface:
In this User Interface module, the user has to give the IP address from which the file should to be transferred. To start the process, the user has to click the click for process button. If the user is an existing user then they shall continue the transfer process by giving their authentication details. If the user is not an existing user then they have to register by giving their details.

2. Transferring Messages
If the client, wants to send a message then the client has to give IP address, subject and the message. If the message is transferred successfully then the client will get the status as "Message Transferred". The message is transferred from client through the nodes. The router takes care of all the nodes. The paths of nodes through which the message is sending are taken and saved. The saved paths then generates

a graph for comparing the existing and proposed energy efficiency, throughput, packet delivery ratio, delay.

3. Static and Dynamic Approach

The router sends the message through nodes based on two approaches such as Static and Dynamic approach. In this module, the user has to enter the IP address and have to select the approach such as Static or Dynamic. Based on these approaches, the router checks the nodes and the node sends the messages. For each approach, the router will create the node's path and generates the route path. The paths checked are then displayed in the router form. Both the approaches provides us the number of paths chosen for sending the message and those paths generates graph for comparing energy efficiency, etc.,

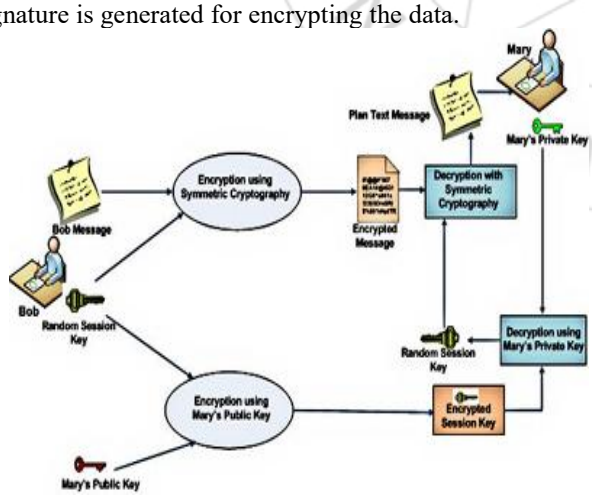
4. Key generation and receiving messages

While the client is sending the message to the receiver, a key is generated. In the receiver side, the receiver has to give the correct key to receive the message. The keys generated in client side and in the receiver side are matched, then the user can receive the message. In this module, the key generation part plays an important role in sending the message securely and efficiently.

4. System Design

Secure communication in SET-IBS relies on ID based cryptography in which user public keys are their ID information. Thus, users can obtain their corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Private key is generated in similar way as that of IBS, Along with private key online signature is generated for encrypting the data.



Wireless Sensor Networks (WSNs) can provide low cost solutions to various real world problems. WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. To consider energy balancing for nodes is an important factor in wireless sensor networks. Many routing, power management and data dissemination protocols have been specifically designed for WSNs where energy consumption is an essential design issue. Owing to the limited resources available for sensor nodes, designing energy efficient routing mechanism to prolong the overall network lifetime has become one of the most important technologies in wireless sensor networks (WSNs).

5. Operations

Secure communication in SET-IBS relies on the ID-based cryptography, information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy

Protocol Initialisation

In this stage let the time stamp for communication between BS to node is denoted by Tbn and let the time stamp for leaf node to CH be denoted by Tlc. The protocol initialisation works in round. In this paper we take IDpk as users public key under IBS scheme, propose a secure data transmission protocol by using IBS mainly for CWSN i.e.., SET IBS. At the initiation of protocol initialisation stage private pairing parameters are preloaded into the sensor nodes so that the node does not have to generate the private key at the initiation of each round required for the authentication of node with another. Upon node becoming the orphan, its ID is distributed to all other nodes by the BS. In this scheme homomorphic encryption scheme is used which allows encryption of the cipher text, thus generating an encrypted result which when decrypted matches the result of the operations performed on plaintext. The BS performs the following operation of key pre distribution in all sensor nodes.

i) Generates the key for encryption required for the homomorphic encryption schemes to encrypt the data messages.
ii) Generate the pairing parameters.
iii) Choose the cryptographic hash functions.
iv) Pick a random integer as master key.
v) Preload each senor node with the public parameters.

Key Management for Security

Let's assume that the sensor leaf node n transmits the message M to the CH I, and encryption is done to the message with the key k done using homomorphic encryption scheme. The cipher text of the message is denoted by C. The SET IBS scheme consists of extraction, signing and verification operations.

$Cn = h(Cn \mid |tn \| \theta n)$

$Ɓn = Cnsekn \| \alpha nP$

Where (σ n, Cn) is the digital signature applied by node n on the encrypted message Cn.

Protocol operation

The protocol operation is done as discussed before that is the setup phase and steady state phase.Setup –Phase: In cluster each node creates a random number with the probability p, each node has the random probability (p) at the each round, and the next round it will creates another probability. Each node generates a random probability (p) at the beginning of a new round and computes the threshold value (T(n)) with

the use of equation (1). If r=1 (i.e. the first round), let EMAX of all nodes be

1) In case of P < PT, the node is selected as a cluster head. A selected cluster head broadcasts an advertisement message over neighbor nodes. The neighbor nodes collect advertised message during a given time interval and then send a "join REQ" message to the nearest cluster head. The cluster head receives the "join-REQ" message and builds a cluster member list schedule. The member node receives and save the message for data transfer.
2) Steady State Phase: In Steady State phase, the operation is divided into frames, in each frame; cluster member nodes send their data to the aggregation node Aggregator according to their time slots. The aggregation node must keep its receiver on to receive all the data from the nodes in the cluster. When all the data has been received, the aggregation node sends it to the base station after performs data aggregation. Cluster head maintains the received information of member nodes. The member nodes will have all the data in the form of TDMA table sent by sink node.

The SET IBOOS is designed for higher energy efficiency. It operates similarly to SET IBS which includes protocol initialisation and operates in round during communication.

a) Protocol Initialization

To minimize the computation and storage cost of signature signing IBOOS scheme is introduced. The protocol initialisation of this scheme is similar to SET IBS. The BS does following operation for SET IBOOS

i) Generates the encryption key with the help of homomorphic encryption scheme.
ii) The PKG selects random generator g of group G and chooses random number as master key.
iii) For each node n randomly select private key generation and H the hash function.
iv) Preload each sensor node with public parameters.

b) Key Management for Security

The node n transmits the message to the destination with time stamp and online signature in the form of ID of the node, time stamp t, offline signature σ and cipher text c.

c) Protocol Operation

The operation of SET IBOOS is similar to SET IBS. It has set up phase and steady state phase as discussed earlier. Earlier Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was used, which is a type of hierarchical clustering, which is self-organising and self-adaptive. It uses each round as a unit, where the rounds are set-up phase and steady state phase as discussed earlier. In LEACH in order to consume equal energy of each node the CH's are rotated from one node to another in the cluster. But providing security to LEACH and similar kind of protocols is difficult as they rearrange the clusters network dynamically, periodically and randomly. So it is difficult to distribute common key and also difficult to provide long lasting node to node relationship. The main disadvantage of LEACH and similar protocols (SecLEACH, RLEACH, GSLEACH) are they use symmetric key management which suffers from an orphan node problem, occurs when node doesn't share its pairwise key with any other node so the node becomes orphan and does not belong to any cluster. In such case the node becomes independent CH without any nodes in its cluster, thus increasing the network energy consumption reducing the network lifetime efficiency. Even if the sensor nodes does not share its pairwise key with the nearest CH but does with the distant CH which requires more energy to transfer the data to the distant CH. To overcome this orphan node problem asymmetric key management is used.

Table 1: Comparison of ID based schemes and other secure transmission protocols

Characteristic	*Secure Data Transmission Protocols*	*ID Based Schemes*
Protocols	LEACH,SecLEACH,GSLEACH,RLEACH,SLEACH	SET IBS, SET IBOOT
Key assigned	Symmetric	Asymmetric
Storage Cost	High	Low
Network Scalability	Low	High
Computational overhead	High	low

6. Conclusion and Future Directions

Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs. The proposed secure data transmission protocols are with concrete ID-based settings, which use ID information and digital signature for verification. Comparing the SETIBS, SET-IBOOS requires less energy for computation and storage. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SETIBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that, using SETIBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

References

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput.Intell. Springer-Verlag, 2010, vol. 278.
[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670,2002
[3] X. H. Wu, S. Wang, "Performance comparison of LEACH and LEACHC protocols by NS2," Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010
[4] P.T.V.Bhuvaneswari and V.Vaidehi "Enhancement techniques incorporated in LEACH- a survey"Department of Electronics Engineering, Madras Institute Technology, Anna University Chennai, India, 2009
[5] Wu Xinhua and Huang Li "Research and Improvement of the LEACH Protocol to Reduce the Marginalization of Cluster Head"Journal of Wuhan University of

Technology Vol. 35, No. 1, Feb. 2011, pp. 79-82, doi:10.3963/j.issn.1006-2823.2011.01.019 (in Chinese).
[6] Tao, L, Zhu, QX, Zhang, L. An Improvement for LEACH Algorithm in Wireless Sensor Network.Proc.5th IEEE Conf. Indust.Electr. Appl. 2010;1:1811-4
[7] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.-Oct. 2010, vol. 02, issue 02, pp. 570-580
[8] Thiemo Voigt, Hartmut Ritter, Jochen Schiller, Adam Dunkels, and Juan Alonso, ". Solar-aware Clustering in Wireless Sensor Networks", In Proceedings of the Ninth IEEE Symposium on Computers and Communications, June 2004