INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 5 ISSUE 2 – MAY 2015 - ISSN: 2349 - 9303

An Efficient Data Transmission for Cluster based Wireless Sensor Networks using TLP Algorithm

R. Karthick[1]
[1]PG Scholar
erkarthickr@gmail.com

A. Pugazhenthi[2]
[2]Assistant Professor
pugal268@email.com

Abstract— In this paper Identity based digital Signature and Identity based online offline algorithm for the cluster based wireless sensor networks is used. Identity based digital signature computes the digital signature signing process. Identity based online offline algorithm reduces the complexity of computational overhead in cluster head. This project reduces the overhead of the cluster head for efficient transmission. The method for efficient data transmission using Identity based digital signature is also implemented for minimizing end-to-end delay using network simulator. The graphics analysis toolbox and awk scripts is used to process the data from trace files.

Index Terms— Cluster based WSNs, ID based digital signature, ID based online offline digital signature, secure data transmission, TLP Algorithm.

1 INTRODUCTION

Cluster based wireless sensor networks consisting of a fixed Base Station (BS) and a large number of wireless sensor nodes are homogeneous in functionality and capabilities. Assume BS is always reliable i.e. the BS is a Trusted Authority. Meanwhile, the sensor nodes may be compromised by attackers and data transmission may be interrupted from attacks on the wireless channel. In a cluster based wireless sensor networks, the nodes are grouped into clusters and each cluster has a Custer Head sensor elected autonomously. Nodes join a cluster depending on the signal strength and distance from base station to transmit the sensed data via cluster head to save energy.

Method of intermediates node CH aggregate data and send it to the BS is preferred than method each sensor node directly send data to BS, but in case of same data transmission it is overhead to cluster head

2 RELATED WORK

Joseph K. Liu et al (2010) proposed an online offline identity based signature scheme for Wireless Sensor Networks (WSN). Due to significant reductions of the cost of computation and storage the scheme is particularly suitable for the WSN environment with severally constrained resources. One of the interesting features of scheme is it provides multi time usage of offline storage allows the signer to reuse the offline recomputed information in polynomial time, in contrast to one time usage in all other online/offline signature schemes.

J. Sun et al (2010) proposed a security system for Vehicular ad hoc Network (VANETs) to achieve privacy desired by vehicles and traceability required by law enforcement authorities. In addition to satisfy fundamental security requirements, including authentication, no repudiation, message integrity, and confidentiality, the proposed privacy preserving defense technique for network authorities handle misbehavior in VANET access[4] .

Sharnil Pandya et al (2014) illustrated Sensor Network history clustering is one of the most effective technique to increase the performance of deployed wireless sensor networks. Along with the implementation of clustering in WSNs it is necessary to resolve numerous challenges like security and efficient data transmission, providing high level security against a variety of security attacks and aggregation of data. It is a challenging task to address all the challenges using a single framework or protocol[1].

Alia Sabri et al (2014) proposed clustering based routing protocol increases scalability of the network, balances energy consumption among the nodes in the network, and reduces the amount of data are actually transmitted to the base station due to the aggregation process. In a single hop mode, all sensor nodes transmit their sensed data directly to the base station or sink without using intermediate nodes, but in a multi hop network, some sensors deliver data to the sink by the assistance of intermediate nodes[6].

Sang Woon et al (2014) proposed a novel predetermined path routing algorithms along with source and destination pair choosing its routing path only among a set of predetermined paths. The scheme proposed an efficient way of distributed construction of predetermined paths and able to distribute traffic over a network. The predetermined path routing algorithms work fully distributed manner with very limited load information or without any load information[2].

Eric Anderson (2014) demonstrates a solution to Spatial reuse Time Division Multiple Access (STDMA) scheduling with reconfigurable antennas. The Joint Beam Steering and Scheduling (JBSS) problem offers both a challenging mathematical structure and significant practical value. The algorithms is for JBSS and describe an implemented system based on time division multiple access[8].

3 PROBLEM DEFINITION

SET-IBS has a protocol initialized prior to the network deployment and operates in rounds during communication stage consists of a setup phase and a steady state phase in each round. The protocol initialized describes the key management of the protocol by using the IBS scheme and the protocol operations afterwards.

The SET protocol for CWSNs using IBOOS protocol is designed with the transmission efficient scenarios for a cluster based

wireless sensor networks with higher efficiency. The proposed Identity based online offline algorithm operates similarly to the previous SET-IBS protocol initialized prior to the network deployment and operates in rounds during communication. First introduce the protocol initialization and then describe the key management of the protocol by using the online offline scheme along with the protocol operations..

4 PROBLEM STATEMENT

Cluster head performs data fusion and transmits data to the BS directly with comparatively high energy. In addition, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and energy is constrained. In CWSNs data sensing, processing, and transmission consume energy of sensor nodes. The cost of data transmission is more expensive than of data processing.

5 KEY MANAGEMENT FOR SECURITY

Assume a leaf sensor node transmits a message to its CH it encrypts the data using the encryption key k from the additive homomorphic encryption scheme and cipher text of the encrypted message is indicated as C. The algorithms of the IBS scheme in CWSNs practically provide the full algorithm in the signature verification. Security is based on the Dynamic Host Protocol (DHP) in the multiplicative group. The IBS scheme in the proposed IBS consists of the following three operations; they are extraction, signing signature, and verification.

In the extraction phase, node first obtains its private key as given in the equation

$$sek_j=H(ID_j||tj)$$

From msk and ID_j, ID_j is its ID, and t_j is the timestamp of node j's time interval in the current round is generated by its CH i from the TDMA control. In signature signing, the sensor node j picks a random number $\alpha_j \in Z^*_q$ and computes ϑ

The sensor node further computes

$$cip= h(ts|q|ID) \quad (1)$$

and

$$\sigma=c(sek)+\alpha P \quad (2)$$

Equation (1) and (2) form (σ,cip) is the digital signature of node on the encrypted message C. The broadcast message is now concatenated in the form of (ID,t,C,σ,c).

Upon receiving the message, each sensor node verifies the authenticity in the following ways: It checks the timestamp of the current time interval t and determines whether the received message is new. Then, if the timestamp is verified, the sensor node further computes $\vartheta_j=e(\sigma_j,P)e(H(ID_j||t_j)-P_{pub})^c$ that is calculated using the timestamp of the current time interval t. The received message is authentic if:

$$\vartheta j=e(\sigma,P)e(H(ID||t)-Ppub)c$$
$$=e(P,P)\alpha =\vartheta \quad (3)$$

If $h(C||t||\vartheta)=h(C||t||\vartheta) = C$ is equal to the received message, the sensor node decides the received message authentic and propagates the data to the next hop. If the verification above fails the sensor node considers the message as either bogus or replaced and ignores it.

6 PROTOCOL OPERATION

IBS and IBOOS protocols provide secure data transmission for CWSNs with concrete ID based settings use ID information and the digital signature for authentication. Both IBS and IBOOS fully solve the orphan node problem from using the Asymmetric key management for CWSNs.

Secure data transmission protocols are with concrete ID based settings, use ID information and the digital signature for verification comparing the IBS, IBOOS requires less energy for computation and storage[2]. Moreover, the IBOOS is more suitable for node to node communications in a cluster based wireless sensor networks since the computation is lighter to be executed.

In IBOOS, the offline signature is executed by the CH sensor nodes. Sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message[4]. Further, the offline sign phase does not use any sensed data or secret information for signing is particularly useful for CWSNs because leaf sensor nodes do not need an auxiliary communication for renewing the offline signature.

After the protocol initialized, IBS operates in rounds during communication. The two rounds in communication phase are setup phase and a steady phase if suppose all sensor nodes know the starting and ending time of each round because of the time synchronization.

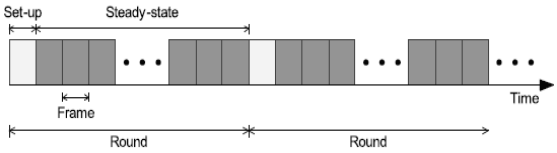

Fig. 1. Operation in Secure Data Transmission

The two phases in the protocol operation is setup phase and steady state phase. The setup phase consists of four steps and steady phase consists of two steps. In the setup phase, the timestamp Ts and node IDs are used for signature generation. In the steady state phase the timestamp tj is used for the signature generation securing the inner cluster communications, and this is used for signature generation securing the CHs to BS data transmission.

At the beginning of setup phase the BS first broadcast its ID, a nonce and the denotation of the starting time Ts of the current node to all sensor nodes for the signature and verification in setup phase.

A sensor node decides whether to become a CH for the current round, based on the threshold T (n) is given in equation

$$T(n) = \frac{\rho}{1-\rho*(r \bmod \frac{1}{\rho})} \cdot \frac{Ecur(n)}{Einit(n)} \qquad \forall n \in Gn \quad (4)$$

Equation computing the threshold T (n) in node n is based on the LEACH protocol[9]. The dynamic clustering algorithm preferably with multiplying the ratio of residual energy of the current sensor node (i.e., (Ecur(n))/(Einit(n))) to increase the energy efficiency in the clustering, Ecur(n) is the current energy and Einit(n) is the initial energy of the sensor node. ρ is the priori determining value stands for the desired percentage of CHs during one round e.g., ρ=10%, r is the current round number and Gn is the set of sensor

nodes not been CHs in the last [1/ρ] rounds. If a value of determined number is less than the threshold the sensor node elects itself as a CH. The sensor node decides to become a CH broadcast if the advertisement message Adv to the neighboring in the network is concatenated with the signature (σ,c).

The sensor node decides to be a leaf node picks a CH to join based on the largest received signal strength of advt messages. Then it communicates with CH i by sending a join request(join) message, It is concatenated with the destination CHs ID IDi, its own IDj, timestamp Ts, and the digital signature (σ,c).

A CH i broadcast an allocation message to its cluster members for communication during the steady state phase yet to be concatenated with the signature[5]. The allocation message includes a time schedule sched IDj|tj for a leaf node . Once the setup phase is over, the network system turns into the steady state phase and data are transmitted from sensor nodes to the BS.

According to the TDMA schedule each leaf sensor node j transmits the encrypted data C in a packet (ID,t,C,σ) to its CH is concatenated with the digital signature in a time slot tj the sender ID with t is the destination identifier for the receiver CH by the way each CH collects messages from all members in its cluster, aggregate and fuses data.

7 EFFICIENT TRANSMISSION ALGORITHM

7.1 IBOOS Algorithm

Step 1: Signature process starts by first extracting the private key from the msk τ and it's identity D.

Step 2: Offline signing at the offline stage, node generates the offline value <σ> with the timestamp of its time slot t for transmission, and store the data for signing online signature when it send the message.

Let X = gτ , then

σj = (Rj,Dj) mod q

Step 3: Online signing at stage node j computes the online signature <σj , Hj> based on the encrypted data Cj and the offline signature σj:

Hj = h(Cj; Dj),

Node i send the message to its destination with t and the online signature, in the form of <D, t, σ, , C>.

Step 4: After receiving the data, each sensor node verifies the authenticity in the following way. It checks the current timestamp t for freshness. If the timestamp is valid, the sensor node further computes the values of gzj and σjRhjj Xhj H(Rj,Dj) mod q, then check if:

gzj = σjRhjj Xhj H(Rj,Dj) mod q

The values of gzj are equal from the received message, the node considers the received message as authentic and accepts it . It also propagates the message to the next node. If the verification above fails the sensor node considers the message as bogus or replaced one or mistaken one then discards it.

7.2. Tri–Level Priority Packet Scheduling Algorithm

In this algorithm we have considered three level queues in the system that is the maximum number of ready queue of a node is three. Priority1 (pri1), Priority2 (pri2) and Priority3 (pri3)queues. Real-time data packets are handled by pri1, the highest priority queue, and processed using FCFS scheme. Non real time data packets that arrive from sensor nodes at levels lower go to pri2, the second highest priority queue. Lastly the non real time data packets that are sensed at a local node go to pri3, the lowest priority queue.

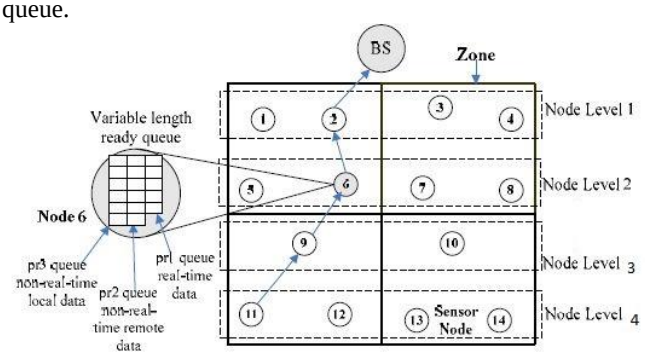

Fig. 2. Tri Level Packet Scheduling

In the TLP scheme the queue size differs based on the requirement of the applications. Preemptive scheduling incurs overhead of context storage and switching in resource constraint sensor networks[7]. The idea behind this scheme is the highest priority tasks are processed with very minimum delay. Non real time packets that arrive from the sensor nodes at lower levels are placed in priority2 queue. Each packet has an ID that consists of Cluster ID and node ID. When two equal priority packets arrive at the same time the data packets generated at lower level have higher priority.

7.3 Pseudo-Code

In this section we propose the pseudo-code of the proposed tri-class priority packet scheduling algorithm.

Algorithm: Tri-level priority data scheduling

while *task* $_{k,I}$ received by node$_i$ at cluster *k* i.e., at *l(k)* **do**

if *task-type*=real-time **then**

put *task*$_k$ in *pri1*queue

if *task*$_k$ is not local **then**

put *task*$_k$ in *pri2* queue // non-real time remote tasks

else

put *task*$_k$ in *pri3* queue // non-real time local task

end-if

else //only two levels

put *task*$_k$ in *pri2* queue // non-real time local task

the duration of timeslot at *l(k)* ← *t(k)*

Therefore remaining time after data sensing,

$t_1(k)$ ← t(k)-senseTime$_k$(t)

if *procTimepri1(K)* ← $\sum_{i=1}^{n(pri)} ProcTime(j)$

end-if

We also consider that each node requires time to sense data packets and also process local or remote data packets[12]. If node has remaining time left while processing real-time data it can process non-real time *pri2* data packets.

8 RESULTS AND DISCUSSION

The extra energy consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed IBS and IBOOS. In order to evaluate the energy consumption of the computational overhead for security in communication, the four metrics for the performance evaluation:

1 .Network lifetime: System energy consumption, and the number of alive nodes. For performance evaluation, compare the proposed IBS and IBOOS with LEACH protocol and SNEP protocol.

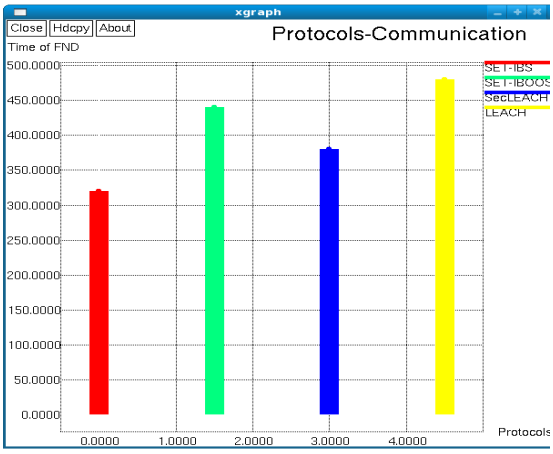

Fig. 3. Time of FND

2. Network lifetime the time of FND: The time of First Node Dies (FND) indicates the sensor network is fully functional. Maximizing the time of FND in a WSN represents to increase the network lifetime.

3. The number of alive nodes: The ability of sensing and collecting information in a WSN depends on the set of alive nodes. Therefore, the evaluation of the functionality of the WSN depends on counting the number of alive nodes in the network.

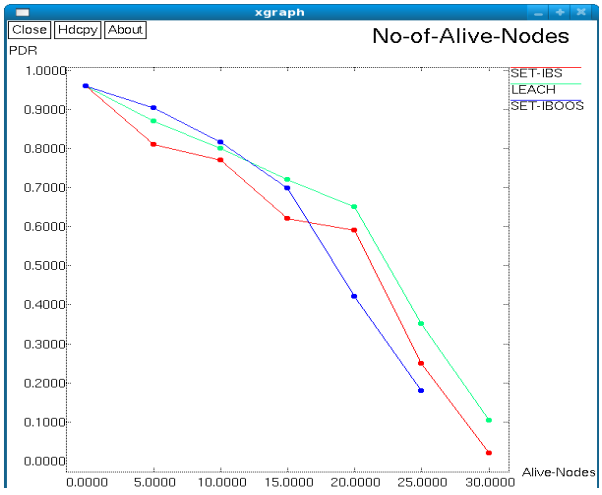

Fig. 4. Number of alive Nodes

4. Total system energy consumption: It refers to the amount of energy consumed in a CWSN before implementing a packet scheduling algorithm. Evaluate the variation of energy consumption in secure data transmission protocols.

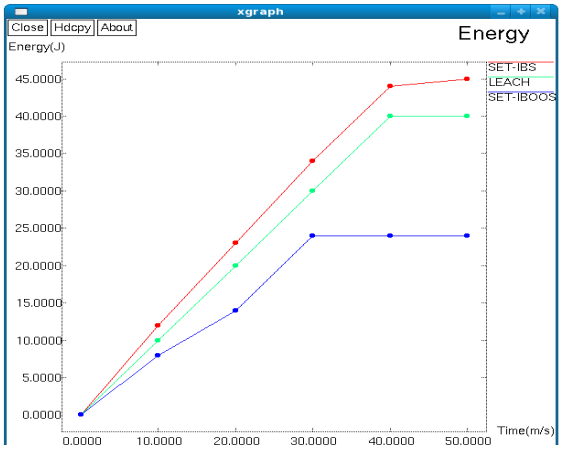

Fig. 5. Energy Consumption of Protocols

5. System energy consumption: It refers to the amount of energy consumed in a CWSN after implementing Tri-class priority packet scheduling algorithm. Evaluate the variation of energy consumption in secure data transmission protocols.

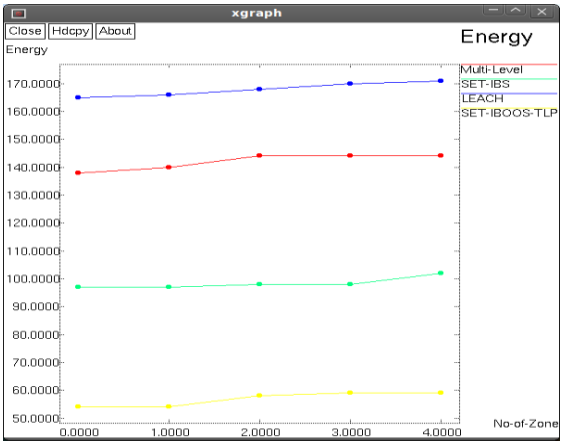

Fig. 6. Energy consumption of TLP algorithm

6. End to End Delay: The average waiting time for data in a network should be less to utilize the full benefit of those data packets. Tri-class priority packet scheduling minimizes end to end delay.

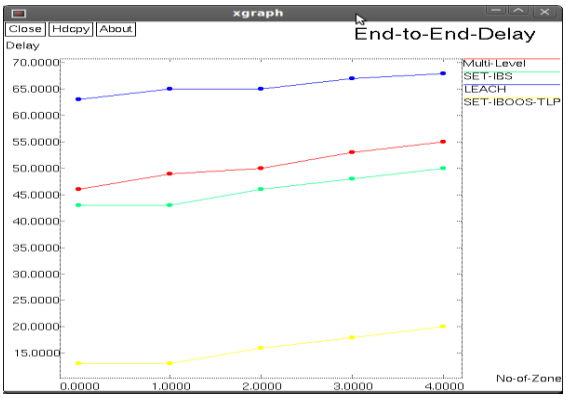

Fig. 7. End-to-End Delay in TLP algorithm

9 CONCLUSION AND FUTURE WORK

Two secure and efficient data transmission protocols for a cluster based wireless network are proposed. Identity based digital Signature and Identity based Online Offline Signature. In the evaluation section, the feasibility of the proposed identity based signature and identity based online offline signature is shown with respect to the security requirements along with finding malicious nodes in the clusters and analysis against routing attacks. Identity based signature and identity based online offline signature are efficient in communication and applying the ID based cryptosystem it achieves security requirements in cluster based wireless sensor networks as well it solves the orphan node problem in the secure transmission protocols with the asymmetric key management. Finally, the comparison in the calculation and simulation results identity based signature and identity based online/offline signature protocols have better performance than existing secure protocols for cluster based wireless sensor networks with respect to both computation and communication costs.

In the future, a unified framework to analyze the sink mobility problem in cluster based wireless sensor networks with congestion detection and avoidance problems is to be studied.

REFERENCES

[1]Banerjee P. and Lahiri S. (2007), 'Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks', Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152.

[2]Boneh D. and Franklin M. (2001), 'Identity Based Encryption from the Weil Pairing', Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01), pp. 213-229.

[3]Even S. and Micali S. (1990), 'On-Line/Off-Line Digital Signatures', Proc. Advances in Cryptology (CRYPTO), pp. 263-275.

[4]Heinzelman W. and Balakrishnan H. (2002), 'An Application Specific Protocol Architecture for Wireless Microsensor Networks', IEEE Trans. Wireless Com, vol. 1, no. 4, pp. 660-670.

[5]Karlof C. and Wagner D. (2003), 'Secure Routing in Wireless Sensor Networks Attacks and Countermeasures', Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315.

[6] Lu H. Li J. and Kameda.H. (2010), 'A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature', Proc. IEEE GLOBECOM, pp. 1-5.

[7]Manjeshwar and Agrawal D.P. (2002), 'An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol', IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302.

[9]Oliveira L.B.(2007), 'SecLEACH On the Security of Clustered Sensor Networks', Signal Processing, vol. 87, pp. 2882-2895.

[10]Pradeepa K. Anne W.R. and Duraisamy S. (2012), 'Design and Implementation Issues of Clustering in Wireless Sensor Networks', Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28.

[11]Sun J et al. (2010), 'An Identity Based Security System for User Privacy in Vehicular Ad Hoc Networks', IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239.

[12]Xu S. Mu Y. and Susilo W. (2006), 'Online Offline Signatures and Multi signatures for AODV and DSR Routing Security', Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110.

[13]Yasmin R. Ritter E. and Wang G. (2010), 'An Authentication Framework for Wireless Sensor Networks Using Identity Based Signatures', Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889.

AUTHOR PROFILE

- R Karthick is currently pursuing master's degree program in computer science and engineering at P. A College of Engineering and Engineering and Technology, Anna University, India. E-mail: erkarthickr@mail.com
- A Pugazhenthi is currently working as an assistant professor in department of computer science and engineering in P. A College of Engineering and Technology, Anna University, India. E-mail: pugal268@gmail.com