International Journal on Applications in Computers
Volume1: Issue 1: May 2018, pp 57- 62 www.aetsjournal.com *ISSN (Online) : XXXX - XXXX*

TLP Algorithm Used Effectively Improves TCP Performance in Data Transmission and Recovery for Cluster Based In WSN

P.SUGANYA.
Assistant Professor, Computer Science and Engineering, A.R Engineering college,Villupuram, Tamilnadu, India. mpsugi@gmail.com

Abstract - TLP's goal is to reduce tail latency of short transactions. It achieves this by converting retransmission timeouts (RTOs) occurring due to tail losses (losses at end of transactions) into fast recovery. TLP transmits one packet in two round-trips when a connection is in Open state and isn't receiving any ACKs. The transmitted packet, aka loss probe, can be either new or a retransmission. When there is tail loss, the ACK from a loss probe triggers FACK/early-retransmit based fast recovery, thus avoiding a costly RTO. In the absence of loss, there is no change in the connection state. Basic of 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 effectively avoids long timeouts and thereby improves TCP performance. The method for efficient data transmission using Identity based digital signature is also implemented for minimizing end-to-end delay using network simulator.

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

1. INTRODUCTION

Retransmission timeouts are detrimental to application latency, especially for short transfers such as Web transactions where timeouts can often take longer than all of the rest of a transaction. This document describes an experimental algorithm, Tail Loss Probe (TLP), to invoke fast recovery for losses that would otherwise be only recoverable through timeouts.

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 [1]. 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 [2]. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

2. RELATED WORKS

The Transmission Control Protocol (TCP) has two methods for recovering lost segments. First, the fast retransmit algorithm relies on incoming duplicate acknowledgments (ACKs), which indicate that the receiver is missing some data. After a required number of duplicate ACKs have arrived at the sender, it retransmits the first unacknowledged segment and continues with a loss recovery algorithm such as the SACK-based loss recovery [RFC6675]. If the fast retransmit algorithm fails for any reason, TCP uses a retransmission timeout as the last resort mechanism to recover lost segments. If an ACK for a given segment is not received in a certain amount of time called retransmission timeout (RTO), the segment is resent [RFC6298].

The contributions of this work are as follows:

- I propose two Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, 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. In the proposed 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 [11].
- SET-IBOOS is proposed to further reduce the computational overhead for security using the IBOOS scheme, in which security relies 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.

- I show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models. Moreover, we compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations, respectively, with respect to both computation and communication[1].
- Lu H. Li J et al (2010) 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 [7].
-

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 [12]. 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 homomorphism 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

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

From msk and ID $_{jj}$, ID_J is its ID, and t 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 a $_j \in Z_{*qj}$ and computes ϑ
The sensor node further computes

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

$$\text{and } s = c(sek) + aP \quad (2)$$

Equation (1) and (2) form (s,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,s,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 furthercomputes $\vartheta_j = e(s_j,P)e(H(ID_j||t_j)-P_{pub})_c$ that is calculated using the timestamp of the current time interval t. The received message is authentic if:

$$\vartheta j = e(s,P)e(H(ID||t)-Ppub)c$$

$$= e(P,P)a = \vartheta \quad (3)$$

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 [1].

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[3]. 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 [5]. 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[1].

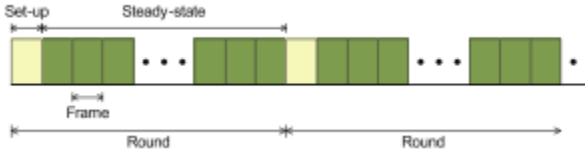

Fig. 1. Operation in Secure Data Transmission

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.

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

$$T(n) = \rho/(1-\rho+(r \bmod \frac{1}{\rho}).(\text{Ecur}(n))/(\text{Einit}(n))) \; \forall n \in Gn \quad (4)$$

Equation computing the threshold T (n) in node n is based on the LEACH protocol [10]. 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 (s,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 (s,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,s) 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. Loss probe algorithm

The Loss probe algorithm is designed for a sender to quickly detect tail losses without waiting for an RTO. I will henceforth use tail loss to generally refer to either drops at the tail end of transactions or a loss of an entire window of data/ACKs.

TLP works for senders with SACK enabled and in Open state, i.e. the sender has so far received in-sequence ACKs with no SACK blocks. The risk of a sender incurring a timeout is high when the sender has not received any ACKs for a certain portion of time but is unable to transmit any further data either because it is application limited (out of new data to send), receiver window (rwnd) limited, or congestion window (cwnd) limited. For these circumstances, the basic idea of TLP is to transmit probe segments for the specific purpose of eliciting additional ACKs from the receiver.

The initial idea was to send some form of zero window probe (ZWP) with one byte of new or old data. The ACK from the ZWP would provide an additional opportunity for a SACK block to det ect loss without an RTO. Additional losses can be detected subsequently and repaired as SACK based fast recovery proceeds. However, in practice sending a single byte of data turned out to be problematic to implement and more fragile than necessary. Instead

we use a full segment to probe but have to add complexity to compensate for the probe itself masking losses[14].

Define probe timeout (PTO) to be a timer event indicating that an ACK is overdue on a connection. The PTO value is set to max(2 * SRTT, 10ms), where SRTT is the smoothed round-trip time [RFC6298], and is adjusted to account for delayed ACK timer when there is only one outstanding segment. TLP MUST NOT be used for non-SACK connections.

7.2. Pseudocode

We define the terminology used in specifying the TLP algorithm:

FlightSize: amount of outstanding data in the network as defined in [RFC5681].

RTO: The transport's retransmission timeout (RTO) is based on measured round-trip times (RTT) between the sender and receiver, as specified in [RFC6298] for TCP.

PTO: Probe timeout is a timer event indicating that an ACK is overdue. Its value is constrained to be smaller than or equal to an RTO.

SRTT: smoothed round-trip time computed like in [RFC6298].

Open state: the sender has so far received in-sequence ACKs with no SACK blocks, and no other indications (such as retransmission (timeout) that a loss may have occurred.

Consecutive PTOs: back-to-back PTOs all scheduled for the same tail packets in a flight. The (N+1)st PTO is scheduled after transmitting the probe segment for Nth PTO.

The TLP algorithm works as follows:

(1) Schedule PTO after transmission of new data in Open state:

Check for conditions to schedule PTO outlined in step 2 below.

FlightSize > 1: schedule PTO in max(2*SRTT, 10ms).

FlightSize == 1: schedule PTO in max(2*SRTT, 1.5*SRTT+WCDelAckT).

If RTO is earlier, schedule PTO in its place: PTO = min(RTO, PTO) [14].

WCDelAckT stands for worst case delayed ACK timer. When FlightSize is 1, PTO is inflated additionally by WCDelAckT time to compensate for a potential long delayed ACK timer at the receiver. The RECOMMENDED value for WCDelAckT is 200ms.

(2) Conditions for scheduling PTO:

(a) Connection is in Open state.
(b) Connection is either cwnd limited or application limited.
(c) Number of consecutive PTOs <= 2.
(d) Connection is SACK enabled.
Implementations MAY use one or two consecutive PTOs.

(3) When PTO fires:

(a) If a new previously unsent segment exists:
−> Transmit new segment.
−> FlightSize += SMSS. cwnd remains unchanged.
(b) If no new segment exists:
−> Retransmit the last segment.
(c) Increment statistics counter for loss probes.
(d) If conditions in (2) are satisfied:
−> Reschedule next PTO.
Else:
−> Rearm RTO to fire at epoch 'now+RTO'.
The reason for retransmitting the last segment in Step (b) is so that the ACK will carry SACK blocks and trigger either SACK-based loss recovery [RFC6675] or FACK threshold based fast recovery [FACK]. On transmission of a TLP, a MIB counter is incremented to keep track of the total number of loss probes sent.

(4)During ACK processing:

Cancel any existing PTO.
If conditions in (2) allow:
-> Reschedule PTO relative to the ACK receipt time.

1. Following is an example of TLP. All events listed are at a TCP sender.
2. Sender transmits segments 1-10: 1, 2, 3, ..., 8, 9, 10. There is no more new data to transmit. A PTO is scheduled to fire in 2 RTTs, after the transmission of the 10th segment.
3. Receives acknowledgements (ACKs) for segments 1-5; segments 6-10 are lost and no ACKs are received. Note that the sender (re)schedules its PTO timer relative to the last received ACK, which is the ACK for segment 5 in this case. The sender sets the PTO interval using the calculation described in step (1) of the algorithm.
4. When PTO fires, sender retransmits segment 10.

5. After an RTT, SACK for packet 10 arrives. The ACK also carries SACK holes for segments 6, 7, 8 and 9. This triggers FACK threshold based recovery.
6. Connection enters fast recovery and retransmits remaining lost segments.

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.

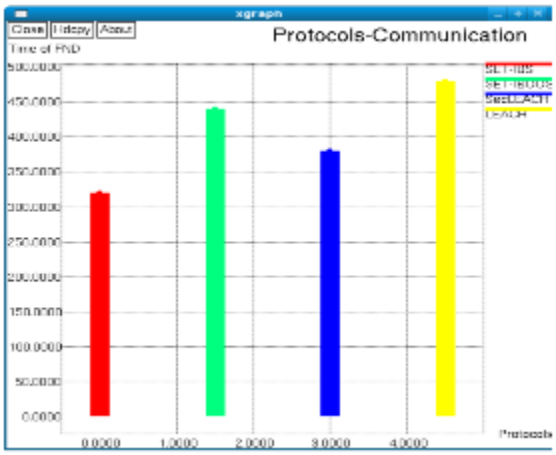

Fig. 2. Time of FND

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. 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.

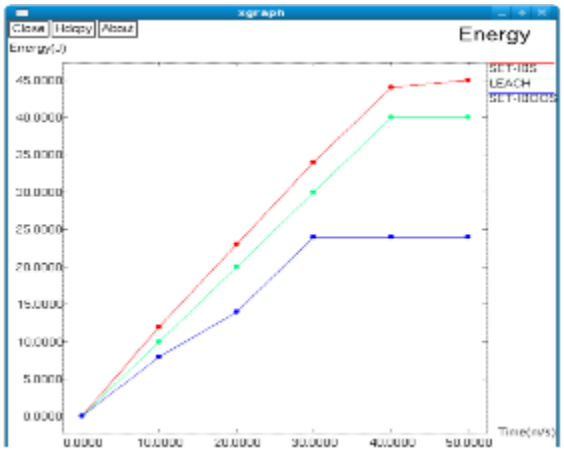

Fig. 3. Energy Consumption of Protocols

4. 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.

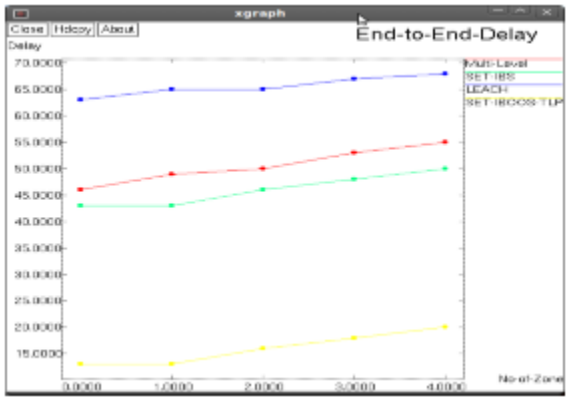

Fig. 4. End-to-End Delay in TLP algorithm

9. CONCLUSION AND FUTURE WORK

Reduce the tail latency of short transmission. It achieves this by converting retransmission timeouts (RTOs) occurring due to tail losses (losses at end of transactions) into fast recovery. TLP transmits one packet in two round-trips when a connection is in Open state and isn't receiving any ACKs. The transmitted packet, aka loss probe, can be either new or a retransmission. When there is tail loss, the ACK from a loss probe triggers FACK/early-retransmit based fast recovery, thus avoiding a costly RTO. Two secure and efficient data transmission protocols for a cluster based wireless network are proposed. 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] Huang Lu, JieLi,Senior and Mohsen Guizani (2014),"Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE Trans. on parallel and distributed systems, Vol. 25, No. 3.

[2] 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.

[3] 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.

[4] Even S. and Micali S. (1990), 'On-Line/Off-Line Digital Signatures', Proc. Advances in Cryptology (CRYPTO), pp. 263275.

[5] Heinzelman W. and Balakrishnan H. (2002), 'An Application Specific Protocol Architecture for Wireless Microsensor Networks', IEEE Trans. Wireless Com, vol. 1, no. 4, pp. 660670.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12]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.

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

[14] Loss probe algorithm (TLP) https://tools.ietf.org/html/draft-dukkipati-tcpm-tcp-loss-probe-01