A Trust-Based Secure Data Aggregation Protocol for Wireless Sensor Networks

Bhavna Arora Makin and Dev Anand Padha***

Generally, the security issues in data aggregation of Wireless Sensor Networks (WSNs) are: data confidentiality and data integrity. Data confidentiality, which protects the sensitive transmitted data from the passive attacks such as eavesdropping, is the basic security issue. Data integrity prevents the compromised source nodes or aggregator nodes from significantly altering the final aggregation value. This paper proposes a trust-based secure data aggregation protocol for WSN. It does not involve any centralized infrastructure. It uses Combined Trust Values (CTVs) to favor packet forwarding for each node. In the proposed scheme, each sensor node has a CTV which is based on the trust evaluation factors, such as identification, sensing data and consistency. Based on these factors, one can identify malicious or compromised nodes, and filter their data from the networks. Each aggregator determines a Message Authentication Code (MAC) value for the aggregated data and finally all the aggregated data reach the sink node. By verifying the MAC value of the aggregators, the sink identifies and eliminates the misbehaving aggregators. The simulation results show that the proposed protocol achieves good delivery ratio and throughput.

Keywords: Security issues, Wireless Sensor Network (WSN), Data aggregation, Trust-based protocol

Introduction

1.1 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) comprise an emerging technology which has received significant attention from the research community. Several small and low cost devices are included in the sensor networks which are self-organizing ad hoc systems. They gather and transmit information to one or more sink nodes by observing the physical environment. Normally, the radio transmission range of the sensor nodes is in the order of magnitude which is smaller than the geographical extent of the entire network. Thus, data needs to be forwarded towards the sink node in a hop-by-hop manner. If the amount of data which needs to be transmitted is reduced, the energy consumption of the network is also minimized (Dorottya and Attila, 2007). A huge number of small electromechanical devices with sensing, computing and communication capabilities are included in WSNs. These devices are utilized to

* Assistant Professor, Model Institute of Engineering & Technology, Kot Bhalwal, Jammu, India; and is the corresponding author. E-mail: barora_makin@rediffmail.com

** Head, Department of Computer Science and IT, University of Jammu, Jammu, India. E-mail: dpadha@rediffmail.com

collect sensory information such as temperature measurements from an extended geographic area (Jukka, 2004).

Active research in the area of sensor networks is performed with the various kinds of possible uses of these networks. Several challenging problems are created due to the characteristics of WSNs (Gregory and Baochun, 2004). The following are some of the characteristics of these networks:

- Sensor nodes are prone to failures;
- Sensor nodes use a broadcast communication paradigm and have stringent bandwidth constraints; and
- Sensor nodes have limited resources.

1.2 Data Aggregation

In WSNs, in order to reduce the medium access layer contention and to achieve energy conservation, data aggregation is considered as one of the fundamental distributed data processing procedures (Zhenzhen *et al.*, 2007). An example for wireless routing in sensor networks is data aggregation. This scheme combines the data coming from the different sources, eliminates its redundancy and reduces the number of transmissions, and thus saves energy (Bhaskar *et al.*, 2002). By using the in-network data aggregation, the inherent redundancy in raw data which is collected from the sensors can be eliminated. Moreover, such operations are utilized for extracting the application-specific information from the raw data. It is crucial for the network to support high incidence of in-network data aggregation for conserving energy for a longer network lifetime (Kai-Wei *et al.*, 2007).

1.3 Threats to Wireless Sensor Networks

WSNs are exposed to several security threats. There is a fair amount of work on threats to WSNs, but it is distributed across various papers. Some of the features of WSNs, such as tree-structured routing, data aggregation, tolerable failures, in-network filtering and computation and phased transmission periods, give rise to threats and challenges (John *et al.*, 2007).

Most network layer attacks against sensor networks fall into any one of the following categories: spoofed, altered or replayed routing information; selective forwarding; sinkhole attacks; Sybil attacks; wormholes; HELLO flood attacks; and acknowledgment spoofing. The work (John *et al.*, 2007) also identifies attacks on specific protocols: TinyOS beaconing; directed diffusion; geographic routing; minimum cost forwarding; low-energy adaptive clustering hierarchy; rumor routing; and energy conserving topology maintenance (GAF, SPAN).

1.4 Secure Data Aggregation

The following are the security issues in data aggregation of WSNs (Yingpeng *et al.*, 2006):

1.4.1 Data Confidentiality

It is the basic security feature that protects the sensitive transmitted data from passive attacks such as eavesdropping. It is important in hostile environments where the wireless channel is vulnerable to eavesdropping. The sensors' power can be used quickly by the complicated encryption and decryption methods like multiplication of large numbers in public key-based cryptosystems, though there are several methods provided by cryptography.

1.4.2 Data Integrity

The compromised source nodes or aggregator nodes are prevented from altering the final aggregation value by data integrity. Since sensor nodes lack expensive tampering-resistant hardware, they can easily be compromised. Moreover, this tampering-resistant hardware will not be reliable every time. A compromised node can modify, copy or discard messages.

Generally, in WSN, the following two methods can be employed for the secure data aggregation:

- Hop-by-Hop Encrypted Data Aggregation: In this scheme, the data is encrypted by the sensing nodes and decrypted by the aggregator nodes. The aggregator nodes then aggregate the data and encrypt the aggregation result again. At last the sink node gets the final encrypted aggregation result and decrypts it.
- End-to-End Encrypted Data Aggregation: In this method, the intermediate aggregator nodes do not have the decryption keys and can only do aggregations on the encrypted data.

The schemes can be compared and evaluated on the evaluation parameters presented in Table 1.

Table 1: Comparison of Data Aggregation Methods

Parameters	Hop-by-Hop Data Encryption	End-to-End Data Encryption
Data Integrity	Provides Maximum Data Integrity	Minimum Data Integrity
Computation Cost	Low	High
Vulnerability to Attacks	More to Passive Attacks	More to Active Attacks
Data Secrecy	Lesser Security	High Security

2. Related Work

2.1 Privacy-Preserving Data Aggregation Schemes for Additive Aggregation Functions

Wenbo *et al.* (2007) have presented two privacy-preserving data aggregation schemes for additive aggregation functions.

Their first scheme is Cluster-based Private Data Aggregation (CPDA) which leverages the clustering protocol and algebraic properties of polynomials within each cluster. The design leverages algebraic properties of polynomials to calculate the desired aggregate value. At the same time, it guarantees that no individual knows the other's data.

Their second scheme is Slice-Mix-AggRegaTe (SMART) which builds on slicing techniques and the associative property of addition. Here, each node hides its private data by slicing it into pieces and then sends encrypted data to different intermediate aggregation nodes. It provides better security compared to CDPA.

The goal of their work is to bridge the gap between collaborative data collection by WSNs and data privacy. They assessed the two schemes by privacy-preservation efficacy, communication overhead and data aggregation accuracy. Their simulation results show the efficacy and efficiency of their schemes.

Prakash *et al.* (2009) have presented a privacy-preserving data aggregation scheme for additive aggregation functions. The goal of their work is to bridge the gap between collaborative data collection by WSNs and data privacy. They have presented simulation results of their schemes and compared their performance to a typical data aggregation scheme TAG, where no data privacy protection is provided. The results show the efficacy and efficiency of their schemes.

Tamer and DaeHun (2009) have presented a dynamic and secure scheme for data aggregation in WSN. Their scheme includes level-based key derivation, data aggregation and new node join phases. Furthermore, they have done a security analysis for a related Level-Based Key Management (LBKM) scheme proposed by Kim and Ramakrishna (2007). Their analysis shows that LBKM is insecure for compromising of one node and misbehavior of neighbor nodes. To this end, they proposed a different level-based key management scheme for secure data aggregation. Their scheme is secure and more efficient than LBKM scheme in terms of communication overhead and security.

2.2 Secure Hop-by-Hop Data Aggregation Protocol

Yi Yang *et al.* (2008) have proposed SDAP, a secure hop-by-hop data aggregation protocol for sensor networks. The designs of SDAP are based on the principles of divide and conquer and commit and attest. The technique first uses a novel probabilistic grouping technique to dynamically partition the node in a tree topology into multiple logical groups (sub-trees) of similar sizes. A commitment-based hop-by-hop aggregation is performed in each group to generate a group aggregate. The base station then identifies the suspicious group based on the set of group aggregates. Finally, each group under suspect participates in an attestation process to prove the correctness of its group aggregates. Moreover, SDAP is a general-purpose secure aggregation protocol applicable to multiple aggregation functions. Their analysis and simulations show that SDAP can achieve the level of efficiency close to an ordinary hop-by-hop aggregation protocol while providing certain assurance on the trustworthiness of the aggregation result.

Shih-I and Shiuhpyng (2007) have proposed a Secure Encrypted-data Aggregation (SEA) scheme in Mobile WSNs (MWSN) environment. Their design for data aggregation eliminates redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission. In contrast to conventional schemes, their proposed scheme provides security and privacy, and duplicate instances of original readings will be aggregated into a single packet; therefore, more energy can be saved.

2.3 An Integrity-Protecting Private Data Aggregation Scheme

Wenbo *et al.* (2008) have presented iPDA, an integrity-protecting private data aggregation scheme. They evaluated the performance of iPDA scheme in terms of communication overhead and data aggregation accuracy by comparing it with a typical data aggregation scheme—TAG, where no integrity protection or privacy preservation is provided. iPDA aims at higher level of data integrity and utilizes node-disjoint aggregation trees in sensor networks. Since each node belongs to a single aggregation tree, a malicious node can only pollute the aggregation result of the aggregation tree it belongs to. The iPDA is achieved through data slicing and assembling technique, and data integrity is achieved through redundancy by disjoint aggregation path trees to collect the data of interest. Their simulation results show that iPDA achieves the design goals while still maintaining the efficiency of data aggregation.

Amrita and Jyoti (2008) have tried to solve the data aggregation problem by building a Secure Aggregation Tree (SAT) having the features of persistent authentication. Firstly, they have described the structure of the SAT. Secondly, when the aggregation values obtained from an aggregation node are in doubt, they proposed a weighted voting scheme to verify whether the aggregation node is behaving well or cheating. A compromised node may forge an aggregation result and mislead base station into trusting a false reading. Efficient and secure aggregation scheme is critical in WSN due to stringent resource constraint. A method was proposed to build the representative-based aggregation tree in WSN, such that sensing data are aggregated along the route from the leaf cell to the root of tree.

3. Security Challenges in Wireless Sensor Networks

Many sensor network routing protocols are quite simple, and for this reason are sometimes susceptible to attacks on routing in *ad hoc* networks. Most network layer attacks against sensor networks fall into one of the following categories (Chris and David, 2003):

- Spoofed, altered, or replayed routing information;
- Selective forwarding;

- Sinkhole attacks;
- Sybil attacks;
- Wormholes;
- HELLO flood attacks; and
- Acknowledgment spoofing.

3.1 Spoofed, Altered or Replayed Routing Information

The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

3.2 Selective Forwarding

In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet it sees. A more subtle form of this attack is when an adversary selectively forwards packets. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable that an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest.

3.3 Sinkhole Attack

In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on or near the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. One motivation for mounting a sinkhole attack is that it makes selective forwarding trivial.

3.4 Sybil Attack

In a Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significant threat to geographic routing protocols.

3.5 Wormhole Attack

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.

Generally, wormholes can be used to exploit routing race conditions. Wormholes are a way to do this, and are effective even if routing information is authenticated or encrypted. Wormholes can also be used simply to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping. Detection is potentially difficult when used in conjunction with the Sybil attack.

3.6 HELLO Flood Attack

A novel attack against sensor networks is the HELLO flood attack. Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) the radio range of the sender. This assumption may be false—a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. An adversary does not necessarily need to be able to construct legitimate traffic in order to use the HELLO flood attack. It can simply rebroadcast overhead packets with enough power to be received by every node in the network. HELLO floods can also be thought of as one-way broadcast wormholes.

'Flooding' is usually used to denote the epidemic-like propagation of a message to every node in the network over a multi-hop topology. In contrast, despite its name, the HELLO flood attack uses a single-hop broadcast to transmit a message to a large number of receivers.

3.7 Acknowledgment Spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgments. Due to the inherent broadcast medium, an adversary can spoof link-layer acknowledgments for 'overheard' packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive. For example, a routing protocol may select the next hop in a path using link reliability. Artificially reinforcing a weak or dead link is a subtle way of manipulating such a scheme. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgment spoofing by encouraging the target node to transmit packets on those links.

4. Methodology

The problems explored in this paper are as follows:

- Due to the algebraic properties of the polynomials, the communication overhead increases and becomes more complex (Prakash *et al.*, 2009).
- The dynamic and secure scheme for data aggregation in WSN is operated only in the tree-based structure. Moreover, the overhead is greater in the case of the threshold cryptography (Tamer and DaeHun, 2009).
- The bandwidth consumption is increased in the case of the SMART technique (Wenbo He *et al.*, 2007).
- The integrity is not discussed in SEA scheme (Shih-I Huang and Shiuhpyng, 2007).
- Also the existing secured schemes on WSNs did not focus on the reduction of energy consumption on cryptographic operations.

4.1 Trust-Based Secure (TBS) Data Aggregation Protocol

We propose a trust-based aggregation scheme in sensor network without using any centralized infrastructure. It uses Combined Trust Values (CTVs) to favor packet forwarding for each node.

In our proposed scheme, each sensor node has a CTV based on the following trust evaluation factors:

- Identification: This factor contains identification information of a node. It consists of a node's location information and node ID.
- Sensing Data: This factor consists of sensing data and sensing time for the events.
- Consistency: This factor represents a level of consistency of a node.

For each node, CTV represents the total trustworthiness of a node, which is evaluated based on the above three factors. Based on these factors, we can identify malicious or compromised nodes, and filter out their data from the network.

A node is punished or rewarded by decreasing or increasing the CTV. Each aggregator marks the packet by adding its hash value to the CTV and forwards the packet towards the destination node. The destination node verifies the hash value and checks the CTV of all nodes. If the hash value is verified, the CTV is incremented, other wise it is decremented. If the CTV falls below a trust threshold, the corresponding node is marked as malicious.

4.1.1 Trust Evaluation Process

To check the trustworthiness of the nodes, the following trust evaluation factors are evaluated:

Identification: This factor contains unique identification information of a node. It consists of a node's position and grid identification in which it is deployed.

$ID_i = < XPosition_i, YPosition_i >$, where $1 \le i \le k$

Sensing Result: This factor represents sensing result information for detected events. This factor consists of sensing data and sensing time for the events.

$SR_i = < SD_i, ST_i >$: Sensing result value of node i, where, $1 \le i \le k$

where SD_i is the sensing data of node i and ST_i is the sensing time of node i.

Consistency: This factor represents the level of consistency of a node. Based on this factor, we can identify malicious or compromised nodes, and filter out their data from the network. The consistency value (CV_i) is given by:

$$CV_i = \frac{CCs_i - ICs_i}{CCs_i + ICs_i}, \text{ where } -1 \le Ci \le 1$$

where CV_i is the consistency value of node i ($1 \le i \le k$), CCs_i is the consistent sensing count of node i, and ICs_i is the inconsistent sensing count of node i.

4.1.2 Trust Estimation

Trust estimation involves an assignment of weights to the trust factors that are evaluated and quantified in trust quantification step. We define W_i as a weight which represents importance of a particular factor from 0 (unimportant) to +1 (most important). The weight is dynamic and dependent on the application.

Hence, the CTV for node i is computed by the following equation:

$$CTV_i = \frac{W_1 ID_i + W_2 SR_i + W_3 CV_i}{\sum_{i=1}^{3} W_i} \quad \ldots(1)$$

where $0 < W_i \le 1$.

As time elapses, trust values for neighbor nodes change dynamically and continuously. If a node makes some trivial and contemporary mistakes in communication or sensing events, it has little influence on the trust value which is evaluated by its neighbor nodes. It is because, each sensor node uses histograms for the accumulative trust evaluation, which are implemented as several count factors in the trust evaluation matrix. Else, if a node broadcasts inconsistent data steadily or seldom communicates with its neighbor nodes, the trust value for that node decreases and gets convergent to –1. Therefore, some malicious or compromised nodes that broadcast inconsistent or deceitful data continuously can be detected and classified in this step.

4.1.3 Aggregator Selection

Prior to a data aggregation, sensor nodes elect an aggregator node in their own grid, which has the highest trust value among all the nodes in an identical grid by the majority of vote. Aggregators can be elected periodically with some application-dependent time interval and changed dynamically. The roles of an aggregator are to get sensing data from member nodes together, output a representative sensing result, and transmit it to the aggregator header. After getting selected as an aggregator, the aggregator node *a* sends its own identification $IDa = < GridID; Position >$ to the sink node and its neighbor nodes.

4.1.4 Data Aggregation

Let $\{CTV_1, CTV_2, \ldots\}$ be the initial trust values of the nodes $\{n1, n2, \ldots\}$ along the route from a source *S* to the sink *D*. Since the node does not have any information about the reliability of its neighbors in the beginning, nodes can neither be fully trusted nor be fully distrusted.

Each aggregator keeps track of the number of packets it has aggregated through a route using a counter (Ct). Each time, when the aggregator *Ak* receives data packets along with the trust value CTV_i from a node *ni*, *Ak* checks the value of CTV_i. If $CTV_i < CTV_{thr}$ (the minimum trust threshold value), then the data packets from the node *ni* will not be aggregated.

If $CTV_i > CTV_{thr}$, then it increments the counter Ctk as:

$$Ctk = Ctk + \alpha \qquad \ldots(2)$$

where α is the number of packets successfully aggregated by *Ak*

Then *Ak* generates a random hash value by computing the MAC over the aggregated data and Ctk with a key shared by the aggregator and the sink, and transmits the MAC to the sink:

$$Ak \xrightarrow{[\text{MAC}(agg, Ctk)]} D$$

Similarly, each aggregator determines its MAC value, and finally all the aggregated data reach the sink *D*.

When the aggregated data from all the aggregators reaches the sink, it checks the counters of the aggregators, before verifying their MAC. The aggregators are considered well-behaving if the counters are greater than a credit threshold C_{thr}. On the other hand, the aggregators are considered misbehaving if the counters are less than C_{thr}. The verifications of the MAC are made only for the misbehaving aggregators instead of verifying all the aggregators, which reduces the control overhead. Also aggregators with counters less than C_{thr} are prohibited from further transmissions.

4.1.5 Steps Involved in the TBS Protocol

```
1. For each sensor node, $S_i$, $i = 1, 2, \ldots, n$
     • Measure the identification factor $ID_i$.
     • Measure the sensing result $SR_i$.
     • Measure the consistency value $CV_i$.
     • Estimate the $CTV_i$.
   End For
2. Choose the aggregator node $A_j$ with the highest $CTV$.
3. For each aggregator $A_j$, $j = 1, 2, \ldots$
     • When $A_j$ receives the data packet from node $S_i$, it measures its trust
       value $CTV_i$.
     • If $CTV_i < CTV_{thr}$, then $A_j$ will not aggregate the packet
       Else:
           $A_j$ aggregates the packet and increments its counter $Ct_j$ as:
               $Ct_j = Ct_j + \alpha$
           where $\alpha$ is the number of packets successfully aggregated by $A_j$.
       End if .
     • $A_j$ generates a random hash value $[MAC(agg, Ct_j)]$.
     • $A_j$ transmits $[MAC(agg, Ct_j)]$ to the sink.
   End For
4. When all the aggregated data from $A_j$ reaches the sink, it checks the counter
   value $Ct_j$.
5. If $Ct_j > C_{thr}$, then;
       $A_j$ is well behaving
   Else:
       $A_j$ is misbehaving
   End if:
6. $A_j$ is prohibited from further transmissions.
```

5. Simulation

5.1 Simulation Setup

The performance of our TBS protocol is evaluated through NS2 (www.isi.edu/nsnam/ns) simulation. A random network deployed in an area of 500 × 500 m is considered.

Initially, 30 sensor nodes are placed in a square grid area by placing each sensor in a 50 × 50 grid cell. Four phenomenon nodes which move across the grid (speed 5 m/s) are deployed to trigger the events. Four aggregators are deployed in the grid region according to our protocol. The sink is assumed to be situated 100 m away from the above-specified area. In the simulation, the channel capacity of the mobile hosts is set to the same value: 2 Mbps. The Distributed Coordination Function (DCF) of IEEE 802.11 is used for wireless LANs as the MAC layer protocol. The simulated traffic is CBR with UDP source and sink. The number of sources is fixed as four around a phenomenon. Table 2 summarizes the simulation parameters used.

Table 2: Simulation Parameters

No. of Nodes	30
Area Size	500 × 500
Mac	802.11
Routing Protocol	DSDV
Simulation Time	50 s
Traffic Source	CBR
Packet Size	50 bytes
Rate	50 bytes
Transmission Range	150 m
No. of Events	4
Speed of Events	5 m/s

5.2 Performance Metrics

The performance of TBS protocol is compared with the non-secure normal aggregation scheme without applying the TBS protocol (hereafter referred to as NoTBS). The performance is evaluated mainly based on the following metrics:

- Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.
- Throughput: It is the number of packets received successfully.
- Drop: It is the number of packets dropped by the legitimate nodes.

5.3 Simulation Results

5.3.1 Based on Attackers

In our initial experiment, we vary the number of attackers as 0, 1, 2 and 3.

Figure 1 gives the packet delivery ratio when the number of attackers is increased. It shows that our proposed TBS protocol achieves good delivery ratio, compared to NoTBS.

Figure 1: Attackers Versus DelRatio

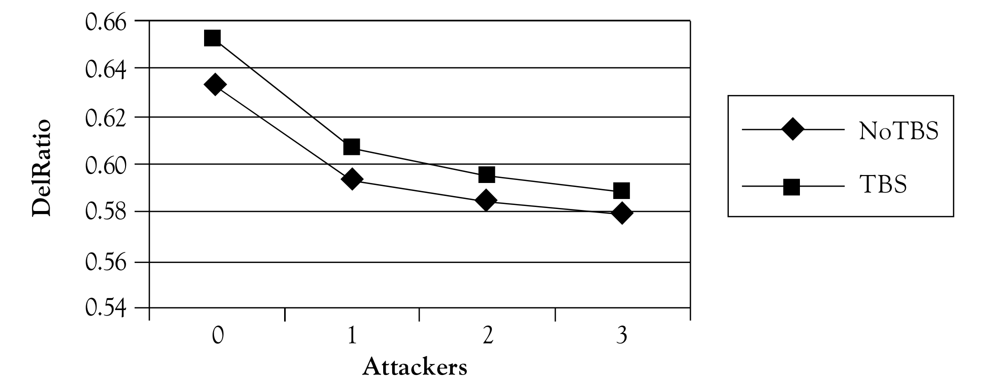


Figure 2 shows the throughput obtained with our TBS protocol, compared with NoTBS protocol. It shows that the throughput is significantly more than the NoTBS, as the number of attackers increases.

Figure 2: Attackers Versus Throughput

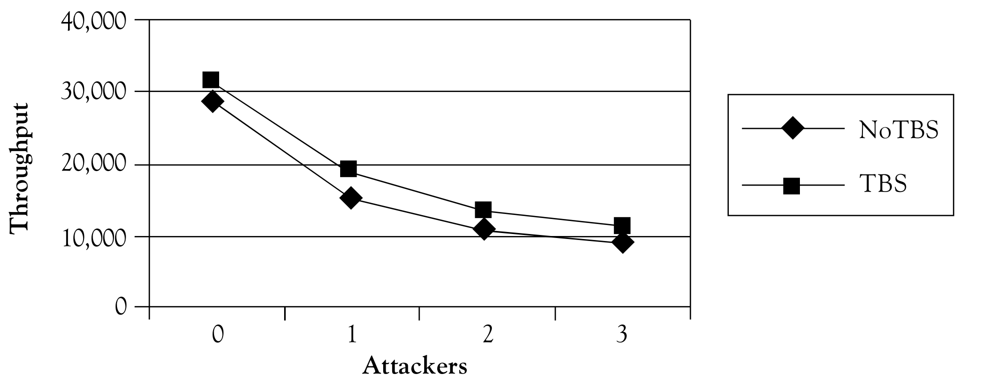


Figure 3 shows the results of packets dropped for the increasing misbehaving nodes. From the results, we can see that TBS protocol has less packets dropped than the NoTBS.

5.3.2 Based on Packet Size

In the second experiment, we vary the packet size as 50, 100, 150, 200 and 250 bytes.

Figure 4 gives the packet delivery ratio when the packet size is increased. It shows that our proposed TBS protocol achieves good delivery ratio, compared to NoTBS.

Figure 5 shows the throughput obtained with our TBS protocol, compared with NoTBS. It shows that the throughput is significantly more than the NoTBS, as the packet size is increased.

Figure 3: Attackers Versus Drop

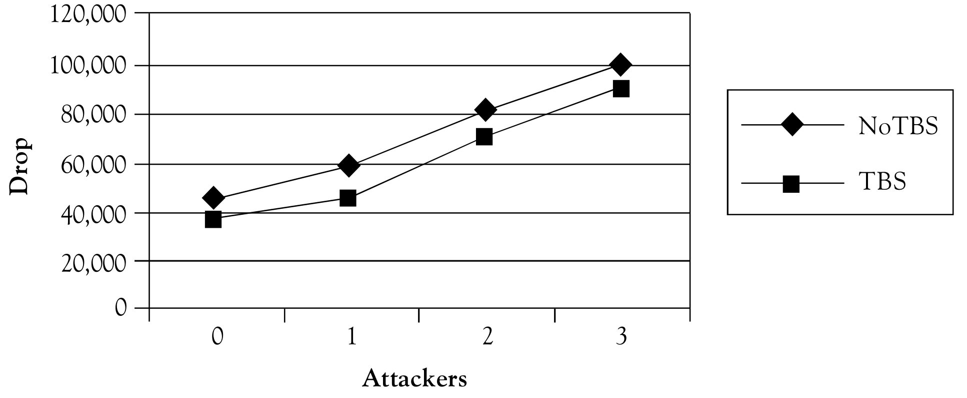


Figure 4: Packet Size Versus DelRatio

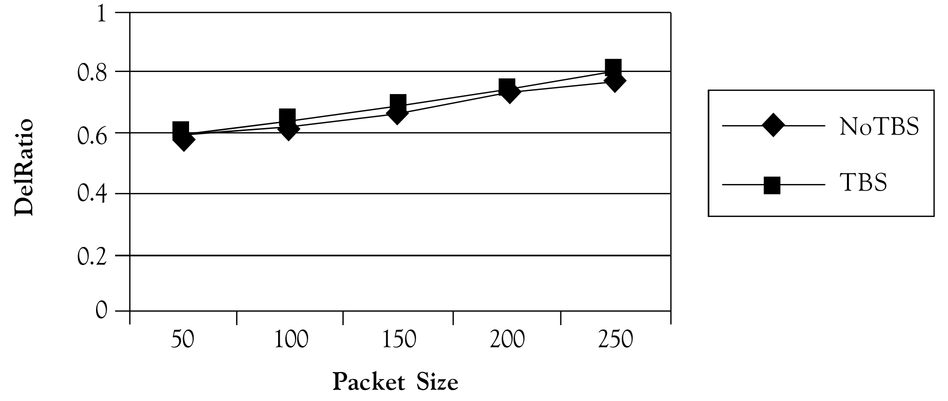
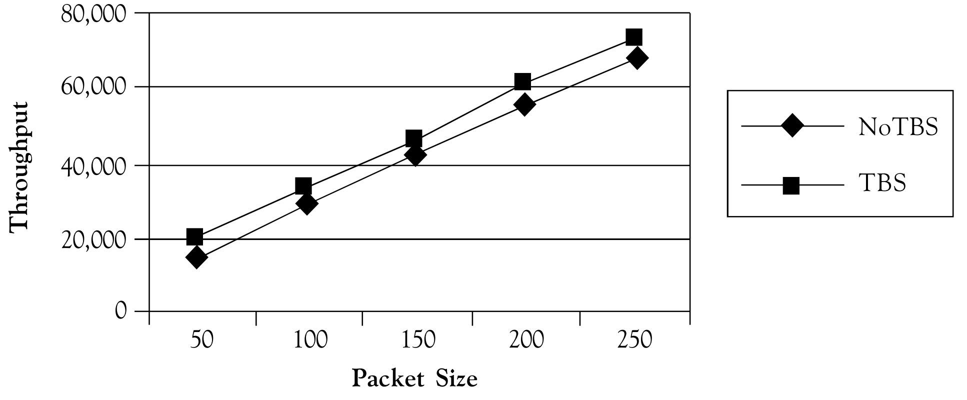


Figure 5: Packet Size Versus Throughput



Conclusion

This paper proposed a trust-based secure data aggregation protocol for sensor networks without using any centralized infrastructure. It uses CTVs to favor packet forwarding for each node. In the proposed scheme, each sensor node has a CTV which is based on the trust evaluation factors such as identification, sensing data and consistency. A node is punished or rewarded by decreasing or increasing the CTV. Each aggregator marks the packets by adding its hash value to the CTV and forwards the packet towards the sink. When the aggregated data from all the aggregators reaches the sink, it checks the counters of the aggregators, before verifying their hash value. The aggregators are considered to be well-behaved if the counters are greater than a credit threshold, otherwise the aggregators are considered to be misbehaving. The verifications of the hash value are made only to the misbehaving aggregators instead of verifying all the aggregators, which reduces the control overhead. Also, the misbehaving aggregators are prohibited from further transmissions. By simulating the results, it has been shown that the proposed protocol achieved good delivery ratio and throughput.

References

1. Amrita Ghosal and Jyoti Prakash Singh (2008), "Secure Data Aggregation Using Some Degree of Persistent Authentication in Sensor Networks", Conference on Mobile and Pervasive Computing (CoMPC), pp. 183-186.

2. Bhaskar Krishnamachari, Deborah Estrin and Stephen Wicker (2002), "The Impact of Data Aggregation in Wireless Sensor Networks", Proceedings of the 22nd International Conference on Distributed Computing Systems, pp. 575-578, IEEE Computer Society, ISBN: 0-7695-1588-6.

3. Chris Karlof and David Wagner (2003), "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications.

4. Dorottya Vass and Attila Vidacs (2007), "Distributed Data Aggregation with Geographical Routing in Wireless Sensor Networks", IEEE International Conference on Pervasive Services, July.

5. Gregory Hartl and Baochun Li (2004), "Loss Inference in Wireless Sensor Networks Based on Data Aggregation", Proceedings of the 3rd IEEE/ACM International Symposium on Information Processing in Sensor Networks (IPSN 2004), pp. 396-404, Berkeley, California.

6. John A Clark, John Murdoch, John A McDermid *et al.* (2007), "Threat Modelling for Mobile Ad Hoc and Sensor Networks", Annual Conference of ITA, September 25-27.

7. Jukka Kohonen (2004), “Data Gathering in Sensor Networks”, Proactive Computing Workshop, November, Helsinki Institute for Information Technology, Finland.

8. Kai-Wei Fan, Sha Liu and Prasun Sinha (2007), “Structure-Free Data Aggregation in Sensor Networks”, *IEEE Transactions on Mobile Computing*.

9. Kim K T and Ramakrishna R S (2007), “A Level-Based Key Management for Both in-Network Processing and Mobility in WSNs”, pp. 1-8, IEEE International Conference Mobile Ad hoc and Sensor Systems (MAHSS).

10. Prakash G L, Manjula S H, Venugopal K R and Patnaik L M (2009), “Secure Data Aggregation Using Clusters in Sensor Networks”, *International Journal of Wireless Networks and Communications*, Vol. 1, No. 1, pp. 93-101.

11. Shih-I Huang, Shiuhpyng Shieh and Tygar J D (2007), “SEA: Secure Encrypted-Data Aggregation in Mobile Wireless Sensor Networks”, *Journal of Wireless Networks*, Vol. 16, No. 4, pp. 915-927.

12. Tamer AbuHmed and DaeHun Nyang (2009), “A Dynamic Level-Based Secure Data Aggregation in Wireless Sensor Network”, *JWIS*, August, pp. 1-11.

13. Wenbo He, Xue Liu, Hoang Nguyen *et al.* (2007), “PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks”, 26th IEEE International Conference on Computer Communications, IEEE INFOCOM.

14. Wenbo He, Hoang Nguyen, Xue Liuy *et al.* (2008), “iPDA: An Integrity-Protecting Private Data Aggregation Scheme for Wireless Sensor Networks in Military Communications Conference (MILCOM), IEEE, November, pp. 1-7.

15. Yi Yang, Xinran Wang, Sencun Zhu and Guohong Cao (2008), “SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks”, *ACM Trans. Inf. Syst. Secur.*, Vol. 11, No. 4, pp. 1-43.

16. Yingpeng Sang, Hong Shen, Yasushi Inoguchi *et al.* (2006), “Secure Data Aggregation in Wireless Sensor Networks: A Survey”, 7th International Conference on Parallel and Distributed Computing, Applications and Technologies.

17. Zhenzhen Ye, Alhussein A Abouzeid and Jing Ai (2007), “Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks”, Draft Infocom Paper.

Reference # 35J-2010-09-01-01