International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 5081-5086

An Attack-Resilient Computation Algorithm for WSNs

Anish Soni[1], Dr. Rajneesh Randhawa[2]

Punjabi University, Patiala(Punjab), India.

Abstract

WSN's are more and more utilized in several applications, like volcano and hearth watching, urban sensing, and border area control. In an extremely massive WSN, in-network information aggregation (combining partial results at intermediate nodes throughout message routing) considerably reduces the quantity of communication overhead and energy consumption. The researcher community projected a loss-resilient aggregation framework known as synopsis diffusion that uses duplicate insensitive algorithms on multipath routing schemes to accurately guess aggregates (e.g., predicate count or sum). However, this aggregation framework doesn't address the matter of false sub-aggregate values contributed by compromised nodes. This attack might cause huge errors within the combination computed at the base station, that is the root node within the aggregation hierarchy. The Proposed system has a tendency to create synopsis diffusion approach secure against the on top of attack launched by compromised nodes. Above all, we have a tendency to present attack-resilient algorithm to modify the leaf nodes to firmly consider predicate count or total even within the presence of such attack. Our attack-resilient computation algorithmic computes actuality combination by filtering out the contributions of compromised nodes within the aggregation hierarchy. Intensive analysis and simulation study show that our algorithmic rule outperforms different existing approaches.

Keywords: NS2, WSN, EEHA, Security, Secure Data Aggregation Protocols

INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth[1]. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. To reduce communication costs, some algorithms remove or reduce node's redundant sensor information and avoid forwarding data that is of no use. As nodes can inspect the data they forward, they can measure averages or directionality for example of readings from other nodes. For example, in sensing and monitoring applications[2], it is generally the case that neighboring sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining.

Although aggregation reduces energy consumption, different attacks[3] on the data falsified the data accuracy . While computing the data, it becomes necessary to find out the compromised nodes. Therefore computation algorithm must be secure enough to resist the attack. We make the synopsis diffusion[4]approach secure against the falsified sub-aggregate attack.

RELATED WORK

Hu & Evans[5] used a lightweight security mechanism for detecting misbehavior in nodes effectively. *SIA[6]* describes a mechanism which resist the stealthy attack. In *ESPDA[7]*, secure communication between nodes was established with very less consumption of energy. Concept of pattern matching was used in which a pattern seed is broadcasted by cluster-head to the sensor nodes and these nodes sent back the corresponding pattern code to the cluster head. S. Rappaport *[8]*, propose signing the data after aggregation to improve the data integrity. In H. Ozgur Sanli et. al. *[9]*, concept of differential data was used and data authentication, confidentiality and freshness was achieved. In *CDA [10]*, aggregation was applied on already encrypted data and for this purpose a homomorphic encryption scheme was used. Yi Yang et. al.*[11]* proposed a protocol that follows the principles of commit/attest and divide/conquer and aggregates the data hop-by-hop. Suat Ozdemir *[12]*, ensures secure data transmission in the presence of compromised nodes. Miloud Bagaa et. al.*[13]* proposed a mechanism in which every node

is capable of immediately verifying the aggregation of the next neighbor and the integrity of its two hops neighbor's data. Hani Alzaid et. al.*[14]* proposed a protocol which integrates reputation system in data aggregation functionalities so as to upgrade the system lifetime and the exactness of aggregated information. A. S. Poornima*[15]* uses end to end privacy for the data. For this purpose, two confidentiality requirements were considered: generic confidentiality and end-to-end confidentiality. Hongjuan Li*[16]*, prevents the disclosure of private data readings sensed by nodes for accurate data aggregation results. The main focus was to defeat eavesdropping attack. Chien-Ming Chen et.al.*[17]* propose a protocol in which data can be recovered even after the completion of aggregation process. Joyce Jose et. al.*[18]* proposed an energy efficient and secure scheme for data aggregation having data freshness, authenticity and privacy. Taochun Wang et. al.*[19]* established a secure channel between the sensor nodes before data transmission. Data was sliced and sent to the neighbors, thus making the transmission more secure.

SYSTEM MODEL

Network Model

We assume that a sensor network consists of a large number of resource-limited sensor nodes which cooperatively accomplish a task. Due to cost constraints these sensors are not equipped with tamper-resistant hardware. In addition, there exists a powerful BS that communicates with the querier which resides outside of the network. In proposed algorithm, the aggregation is performed over an aggregation tree rooted at the BS. There are three types of nodes in the sensor network: base station, intermediate nodes, and leaf nodes. The base station is the node where aggregation result is destined. An intermediate node serves as an aggregator node, which is responsible for forwarding queries, aggregating the received data and its own sensor reading, and then forwarding the new result to its parent. The leaf nodes adopt the ''slicing, mixing, counting and sum" technique to protect privacy; thus, they are responsible for decomposing their primitive data into pieces, sending the pieces to different neighbors, then assembling the received slices to get new results, and sending the new results to their parents.

Attack Model

We mainly focus on the defense of eavesdropping to protect data privacy in wireless sensor networks. In an eavesdropping attack, an attacker tries to overhear the transmission over wireless links to obtain private information. We assume that the attacker may know the security mechanisms that are deployed in a sensor network; he may be able to compromise a node through the radio communication channel. Each node's data should be only known to itself. Such attacks make private data released to adversaries, threatening the privacy of data held by individual sensor nodes.

Slicing:

We adopt the slicing technique proposed in existing system. First, each leaf i of the tree randomly selects a set of nodes within h hops. For a dense sensor network, we can take h= 3. We define that the leaf itself is one element of Si. The primitive data sensed by node i is denoted by vi. Leaf i then slices its private data vi randomly into K pieces, which means that the summation of K pieces is equal to vi. Where one of the K pieces is kept at node i itself, the remaining K-1 pieces are sent to nodes in Si, we take h= 3 here.. We denoted ij as a piece of data sent from node i to node j.

Mixing:

First, all leaves of the aggregation tree wait for certain time, which guarantees that all slices are received, sums up all the received slices and the slice left by itself to get an aggregated result.

Count:

In this, each node X generates a local synopsis QX which is a bit vector of length $\eta > \log N$, where N is the upper bound on Count. To generate QX, node X executes the function Coin Toss(X, η), where X is the node's identifier. It can be interpreted as a coin-tossing experiment with a hash function. The function hash Of () whose output is 0 or 1 simulates a fair coin-toss.

Sum:

The Count algorithm can be extended for computing Sum. The synopsis generation function SG() for Sum is a modification of that for Count, while the fusion function SF() and the evaluation function SE() for Sum are identical to those for Count. Note that Count can be considered as a special case of Sum where each node's sensor reading is equal to one unit. Furthermore, S is the Sum of the sensed values of the nodes present in the Network.

Computing Sum despite Attacks:

In this module, we develop an attack-resilient protocol which enables BS to compute the aggregate despite the presence of the attack. We observe that, in general, BS can verify the final synopsis if it receives one valid MAC for each '1' bit in the synopsis. In fact, to verify a particular '1' bit, say bit i , BS does not need to receive authentication messages from all of the nodes which contribute to bit i . As an example, more than half of the nodes are likely to contribute to the leftmost bit of the synopsis, while to verify this bit, BS needs to receive a MAC only from one of these nodes.

PROPOSED SCHEME:

Sensor nodes collects data from the environment and pass it to aggregator node which calculates the aggregate and further

pass the result to base station as shown in Figure 1.

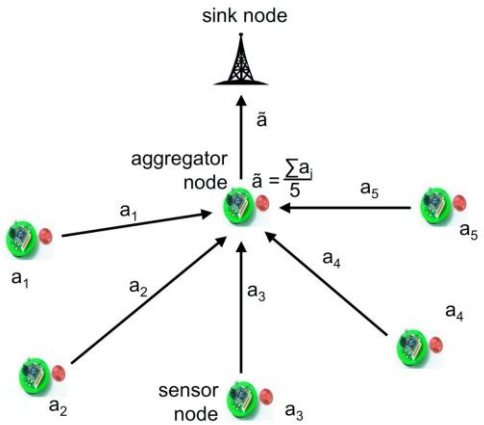

Figure 1: System Architecture

We design an algorithm to securely compute aggregates, such as Count and Sum despite the falsified sub-aggregate attack. In particular, our algorithm which we call the attack-resilient computation algorithm consists of two phases. In the first phase, the BS derives a preliminary estimate of the aggregate based on minimal authentication information received from the nodes. In the second phase, the BS demands more authentication information from only a subset of nodes while this subset is determined by the estimate of the first phase. At the end of the second phase, the BS can (locally) filter out the false contributions of the compromised nodes from the aggregate. Different steps of algorithm are shown in Figure2.

The key observation which we exploit to minimize the communication overhead is that to verify the correctness of the final synopsis (representing the aggregate of the whole network) the BS does not need to receive authentication messages from all of the nodes.

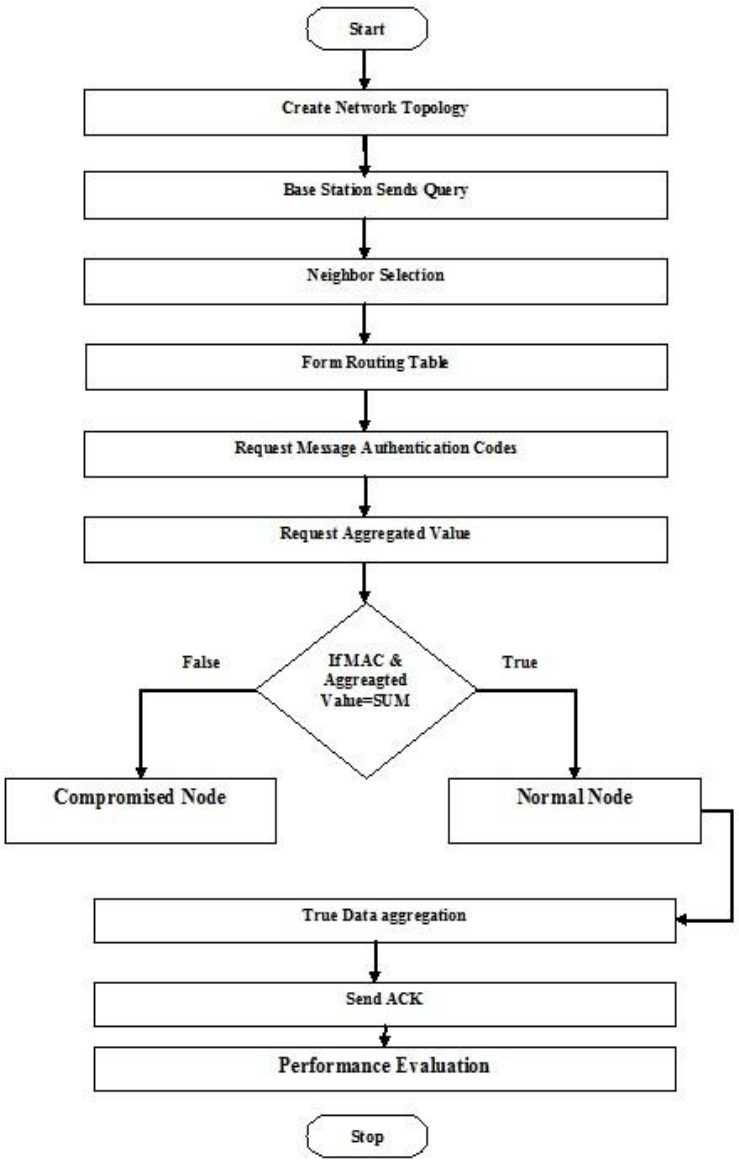

Figure 2: Steps in attack-resilient computation algorithm

SIMULATION SCENARIO

Our protocol is implemented using NS2 and OTCL Language. A Linux PC with i3 Processor and 2GB RAM is used for simulation. Network of 24 sensor nodes is deployed randomly . The maximum range over which a node can transmit the data is 50 m.. The energy consumed in transmitting 1 bit of data is assumed to be 1.23µ Joules and for receiving same amount of data, this consumption is 0.98µ Joules. For sensing 1 bit of data, energy consumption is assumed to be 0.050µ Joules. Simulation setup is shown in figure 3.

```
#    Simulation parameters setup
#============================
set val(chan)  Channel/WirelessChannel   ;# channel type
set val(prop)  Propagation/TwoRayGround  ;# radio-propagation model
set val(netif) Phy/WirelessPhy           ;# network interface type
set val(mac)   Mac/802_11                ;# MAC type
set val(ifq)   Queue/DropTail/PriQueue   ;# interface queue type
set val(ll)    LL                        ;# link layer type
set val(ant)   Antenna/OmniAntenna       ;# antenna model
set val(ifqlen) 50                       ;# max packet in ifq
set val(nn)    24                        ;# number of mobilenodes
set val(rp)    DSDV                      ;# routing protocol
set val(x)     1897                      ;# X dimension of topography
set val(y)     437                       ;# Y dimension of topography
set val(stop)  40.0                      ;# time of simulation end
```

Figure 3: Simulation Setup

PERFORMANCE ANALYSIS:

Communication Overhead

In wireless sensor networks, energy consumed in data transmission is much more than computation. Communication overhead can be determined by the number of transmissions which takes place in a given time period. Larger the number of transmissions, higher is the communication overhead. Simulation shows that our algorithm outperforms the existing EEHA algorithm. But We declare that the communication overhead of our algorithm might be higher if the assumption about compromised nodes being uniformly distributed does not hold.

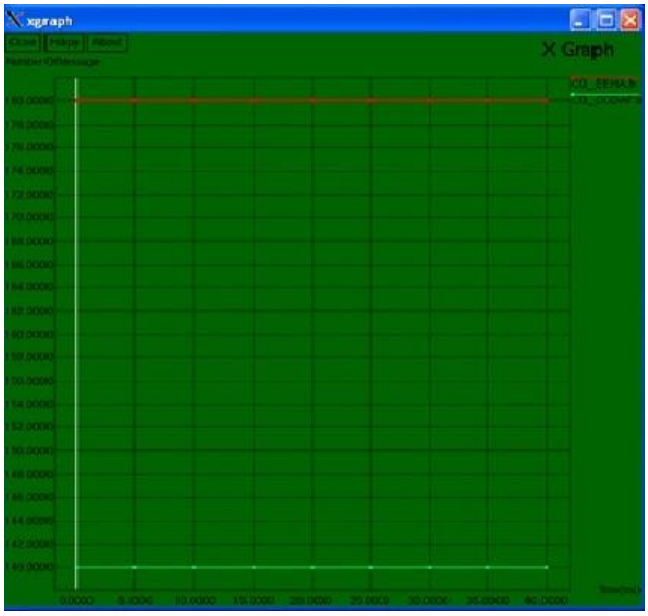

Figure 4: Comparison of Communication Overhead

Aggregation Accuracy

Data which finally sent to the base station is of no importance if it is not accurate. Achieving aggregation accuracy in the presence of compromised nodes is a big challenge for the researcher community. In existing EEHA scheme, accurate data aggregation is achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors. We design an algorithm to securely compute aggregates, such as Count and Sum despite the falsified sub-aggregate attack. Simulation shows that proposed algorithm gives better accuracy even in the presence of compromised nodes.

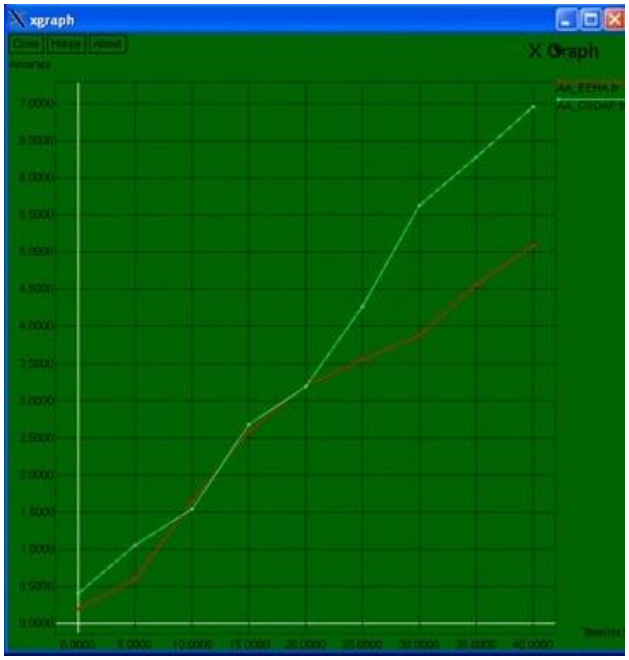

Figure 5: Comparison of Aggregation Accuracy

Energy Consumption:

Wireless sensor network nodes operate on limited battery power , therefore energy consumption of sensor nodes is a very important factor which must be taken into consideration while designing the network. The Figure 6 shows the comparison of energy consumption of existing and proposed protocol and it can be seen that after the end of simulation more energy is left behind in proposed algorithm.

Figure 6: Comparison of Energy Consumption

CONCLUSION

We discussed the security issues of in-network aggregation algorithms to compute aggregates such as predicate Slicing, Mixing, Count and Sum. In particular, we showed the falsified sub-aggregate attack launched by a few compromised nodes can inject arbitrary amount of error in the base station's estimate of the aggregate. We presented an attack-resilient algorithm in Wireless Sensor Networks which would guarantee the successful computation of the aggregate even in the presence of the attack.

REFERENCES

[1] M. Liu, N. Patwari, and A. Terzis, "Scanning the issue," Proc. IEEE, vol. 98, no. 11, pp. 1804–1807, Apr. 2010.

[2] T. Ko, J. Hyman, E. Graham, M. Hansen, S. Soatto, and D. Estrin, "Embedded imagers: Detecting, localizing, and recognizing objects and events in natural habitats," Proc. IEEE, vol. 98, no. 11, pp. 1934–1946, Nov. 2010.

[3] C. Karlof and D. Wagner," Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *AdHoc Networks Journal*, Volume 1, no. 2–3,pp. 293–315, September 2003.

[4] 4.S. Nath, P. B. Gibbons, S. Seshan, and Z. Anderson, "Synopsis diffusion for robust aggregation in sensor networks," in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst. (SenSys), 2004, pp. 250–262.

[5] Hu L., Evans D., "Secure Aggregation for Wireless Networks", in *International Symposium on Applications and the Internet* ,Orlando, Florida, USA, pp. 384-391, 27-31 January 2003.

[6] Przydatek B., Song D., Perrig A., "SIA: Secure Information Aggregation in Sensor Networks", in proceedings of the *1st International Conference on Embedded Networked Sensor Systems*, Los Angeles, CA, USA, pp. 255-265, November 05 – 07, 2003.

[7] Cam H. et al. , "ESPDA: Energy-Efficient and Secure Pattern-Based Data Aggregation for Wireless Sensor Networks", in *Computer Communications, Elsevier*, Volume 29, Issue 4, pp. 446–455, February 2006.

[8] Mahimkar A., Rappaport T. S., "SecureDAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks", in *IEEE Conference on Global Telecommunications*, Volume 4, pp. 2175-2179,29 Nov. – 3 Dec. 2004.

[9] OzgurSanli H., Ozdemir S., Cam H., "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks", in *IEEE 60th Conference on Vehicular Technology*, VTC2004-Fall, Volume 7, pp. 4650–4654, 26-29 September 2004.

[10] Girao J., Schneider M., Westhoff D., "CDA: Concealed Data Aggregation in Wireless Sensor Networks", in *IEEE International Conference on Communications*, Volume 5, pp. 3044-3049, 16-20 May 2005.

[11] Yang Y. et al., "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks", in *Journal of ACM Transactions on Information and System Security (TISSEC)*, Volume 11, Issue 4,Article No. 18, New York, USA, July 2008.

[12] Ozdemir S., "Secure and Reliable Data Aggregation for Wireless Sensor Networks", in proceedings of *4th International Symposium, UCS 2007,* Tokyo, Japan, pp. 102-109, 25-28 November 2007,.

[13] Bagaa M. et al., "SEDAN: Secure and Efficient Protocol for Data Aggregation in Wireless Sensor Networks", in proceedings of *32nd IEEE Conference on Local Computer Networks,* pp. 1053-1060, 15-18 October 2007.

[14] Alzaid H., Foo E., Nieto J. G., "RSDA: Reputation-based Secure Data Aggregation in Wireless Sensor Networks", in proceedings of *9th IEEE International Conference on Parallel and Distributed Computing, Applications and Technology*, pp. 419-424, 1-4 December 2008.

[15] Poornima. A. S., Amberker B. B., "SEEDA: Secure

End-to-End Data Aggregation in Wireless Sensor Networks", in proceedings of *7th IEEE International Conference on Wireless and Optical Communications Networks (WOCN)* , pp. 1-5, 6-8 September 2010.

[16] Li H., Lin K., Li K., "Energy-Efficient and High-Accuracy Secure Data Aggregation in Wireless Sensor Networks", in *Journal of Computer Communications, Elsevier*, Volume 34, Issue 4, pp. 591–597, 1 April 2011.

[17] Chen C. M. et al., "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", in *IEEE Transactions on Parallel and Distributed Systems*, Volume 23, Issue 4, pp. 727-734,August 2011.

[18] Jose J., Princy M., Jose J., "PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks", in *IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology*, pp. 330-336, 25-26 March 2013.

[19] Wang T., Qin X., Liu L., "An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks" in *International Journal of Distributed Sensor Networks, Hindawi Publications*, Article ID 843485, Volume 2013(2013).