International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on Straining Attacker‟s Impact in WSN using Secure Data Aggregation

Devendra Hapase[1], S. D. Satav[2]

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar, Pune-28, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

[2]Assistant Professor, M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar, Pune-28, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

Abstract: ***A Wireless Sensor Network can be defined as a group of sensors which are distributed spatially to monitor physical or spatial conditions such as temperature, volcano, fire monitoring, sound, urban sensing, pressure etc. In a large WSN, the data aggregation significantly reduces communication overhead and energy consumption. In order to pass data, although data in-network aggregation was used and it reduced the problem of communication overhead and transmission loss but failed in computing double-counting sensitive aggregates at the Base Station. The research community proposed synopsis diffusion to eliminate this problem but it did not helped in securing the network against the problem of attacks caused by the compromised nodes, resulting in the false computation of aggregate. In this paper, synopsis diffusion is being made secure against the attacks by compromised nodes. To do so, an algorithm is being presented which can securely compute aggregates in the presence of such attacks. This algorithm is named as Attack-Resilient algorithm. The attack-resilient algorithm computes the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy. Extensive studies and performance analysis have shown that the proposed algorithm i.e. Attack-Resilient algorithm is more effective and outperforms other existing approaches.***

Keywords: Data aggregation, hierarchical aggregation, in-network aggregation, sensor network security, synopsis diffusion, attack resilient.

1. Introduction

Wireless Sensor Networks (WSNs) are increasingly used in several applications, such as wild habitat monitoring, forest fire detection, and military surveillance. After being deployed in the field of interest, sensor nodes organize themselves into a multihop network with the base station as the central point of control. Typically, a sensor node is severely constrained in terms of computation capability and energy reserves.

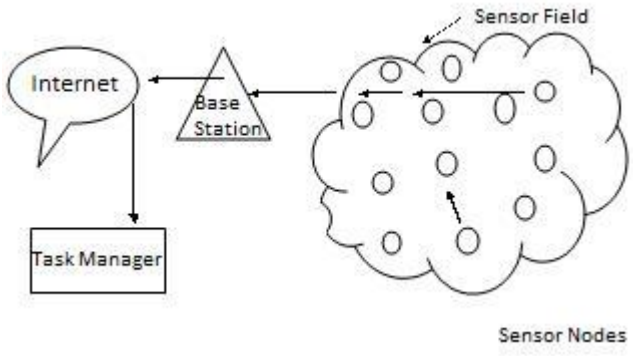

Figure 1: Communication Architecture for WSN

A straightforward method to collect the sensed information from the network is to allow each sensor node‟s reading to be forwarded to the base station, possibly via other intermediate nodes, before the base station processes the received data.

In large WSNs, computing aggregates *in-network* (i.e., combining partial results at intermediate nodes during message routing) significantly reduces the amount of communication and hence the energy consumed. An approach used by several data acquisition systems for WSNs is to construct a spanning tree rooted at the base station, and then perform in-network aggregation along the tree.

The important aggregates considered by the research community include Count, and Sum. Note that it is straightforward to generalize these aggregates to predicate Count (e.g., number of sensors whose reading is higher than 100 unit) and Sum. Furthermore, Average can be computed from Count and Sum. A Sum algorithm can be also extended to compute Standard Deviation and Statistical Moment of any order. Tree-based aggregation approaches are not resilient to communication losses resulting from node and transmission failures, which are relatively common in WSNs. To address this problem, the research community has proposed the use of multipath routing techniques for forwarding sub aggregates. For aggregates such as Min and Max, which are duplicate-insensitive, this approach provides a fault-tolerant solution. However, for duplicate-sensitive aggregates, such as Count and Sum, multipath routing leads to double-counting of sensor readings. Recently, several researchers have presented clever algorithms to solve the double-counting problem associated with multipath approaches. A robust and scalable aggregation framework called synopsis diffusion has been proposed for computing duplicate-sensitive aggregates, such as Count and Sum. This approach uses a ring topology where a node may have multiple parents in the aggregation hierarchy, and each sensed value or sub aggregate is represented by a duplicate-insensitive bitmap called *synopsis*.

However, most of the existing in-network data aggregation algorithms have no provisions for security. A compromised node might attempt to thwart the aggregation process by

launching several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on. This paper focuses on one of the most vexing attacks: the *falsified subaggregate attack*, in which a compromised node relays a false subaggregate to the parent node with the aim of injecting error to the final value of the aggregate computed at the base station. In this approach, an algorithm is designed to compute aggregates, such as Count and Sum, and to enable the base station to verify if the computed aggregate is valid. This algorithm is called the *verification algorithm*, though strictly speaking, it is an aggregate computation and verification algorithm. The key observation is to minimize the communication overhead of this algorithm is that to verify the correctness of the final synopsis (the aggregate of the whole network) the base station does not need to receive authentication messages from all of the nodes. The performance of algorithm is validated via both theoretical analysis and simulation. Irrespective of the network size, the per-node communication overhead in verification algorithm is , while that of the least expensive existing algorithm is , where is the value of the aggregate, Count or Sum. It is to be noted that while algorithm is designed having WSNs in mind, it is straightforward to extend our solution for secure aggregation query processing in a large-scale distributed database system over the Internet.

2. Technical Keywords

1. Data aggregation: A Wireless Sensor Network (WSN) typically consists of a sink node sometimes referred to as a Base Station and a number of small wireless sensor nodes. The base station is assumed to be secure with unlimited available energy while the sensor nodes are assumed to be unsecured with limited available energy. The sensor nodes monitor a geographical area and collect sensory information. Sensory information is communicated to the Base Station through Wireless hop by hop trans- missions. To conserve energy this information is aggregated at intermediate sensor nodes by applying a suitable aggregation function on the received data. Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes

2. WSN: A wireless sensor network (WSN) 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 more modern networks are bi-directional, also enabling control of sensor activity.
control of sensor activity.

3. Synopsis Diffusion: Synopsis Diffusion addresses the problem of robustly comput- ing aggregates (e.g., the average temperature reported by the sensors) in a wireless sensor network. Traditional approaches for computing aggregates use in-network ag- gregation over a spanning tree rooted at the base station. However, a tree, being fragile against node- and communication-failures, gives inaccurate answers in practice. For example, under a message loss rate (20-30 percent) typical in real sensor deploy- ments, the inaccuracy can be as high as 75 percent. One way to make the routing robust is to employ redundancy, by using multi-path routing for example. However, using such redundancy with traditional in-network aggregation approaches would introduce double-counting because sensor readings and partial results would be sent along multiple paths. This concern with double-counting led the researchers to stick with the tree topology despite its inaccuracies

3. Literature Survey

In wireless sensor network security is a big challenge because sensor nodes are deployed in hostile environment, vulnerable to physical attacks and can be compromised by an attacker. Data aggregation in WSN is also an important issue for security to maintain the data confidentiality, data integrity, data freshness, data authentication. Various approaches for secure data aggregation are described as:

In Secure Information Aggregation (SIA) [6], various approaches are used such as "aggregate-commit-prove" in this approach aggregator"s help for computing aggregated data of various sensor nodes reading and to base station with aggregated result to gather with a commitment to collection of data and home server (BS) can verify the correctness of data. This paper provided technique for securely computing the median, minimum and maximum values, average of measurements. This protocol need only sub-linear communication between aggregator and user, proposed a scheme for forwarding secure authentication to confirm that there is no change in sensor previous reading the sensor has recorded, even if an attacker corrupts sensor nodes at a point. In a Tiny Aggregation Service (TAG) [7], this is data aggregation service without any provision for security. This paper proposed aggregation in low-power, distributed, wireless environment. This approach provided two attribute: first, it provided a basic, declarative, medium for data gathering and aggregation which is inspired by selection and aggregation facilities in data base query language. Second, it distributes executes aggregation queries in the sensor network. It is sensitive to lossy communication and resource constrained properties of WSN. This service discards irrelevant data and combines relevant data into more compact records.

In Synopsis Diffusion for Robust Aggregation in Sensor Networks [8], this paper designed an aggregation framework called synopsis diffusion. This is in network aggregation scheme and it avoids double counting by using "order-and duplicate-insensitive (ODI) synopses" that summarize intermediate result. Both ODI synopsis and synopsis diffusion has the property of creating elusive acknowledgement of packet delivery.

In A Secure Hop-by Hop Data Aggregation Protocol (SDAP) [9], this protocol is based on "divide and conquer and commit and attest" principles. First to divide the sensor nodes in a tree topology of similar sizes it used a novel probabilistic grouping technique. For security reason base station identifies the dishonest groups which are based on the set of group aggregates. This protocol is applicable to multiple aggregation function.

In A Secure Data Aggregation and verification Protocol (SDAV) [10], this paper designed two sub-protocols. First protocol used verifiable secret sharing of cluster keys in sensor network by using Elliptic Curve Cryptography (ECC). Second, designed Secure Data Aggregation and Verification Protocol. In this protocol base station never accepts false aggregate data and by using Merkle Hash Trees, it checks integrity of data.

In Secure and Efficient protocol for Data Aggregation (SEDAN) [11], this paper developed two hops verification mechanism for data integrity. This scheme does not require base station to verify and detect mistakes in aggregated results, and each node can verify integrity of data of two hops away neighbors and aggregation of immediate neighbors. This scheme is beneficial to avoid useless transmission of bogus data and saves energy of sensor nodes.

In Reputation-based Secure Data Aggregation (RSDA) [12], this paper focused on data availability and data accuracy. By integrating aggregation functionalities it enhance the network lifetime and accuracy of aggregated data. The area is divided into smaller cells of equal size where RSDA is implemented. In order to filter out the inconsistent data in presence of multiple compromised nodes, each sensor nodes evaluates the behavior of its cell member by monitoring neighborhood"s activities. This approach is required to detect compromised nodes and black list them and helps to extend network life time and protect the accuracy of aggregated data.

In Secure Hop-by-Hop Aggregation of End-to-End Concealed Data [13], this paper presented an efficient heuristic approach for checking data integrity and cost effective heuristic based divide and conquer (declared to be true) process, which has complexity O (ln n) in average, and O(n) in the worst case. In this approach base station used O (1) heuristic to verify final aggregation data.

Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks [14] this paper represents a novel way to provide confidentiality and integrity preserving aggregation in wireless sensor network. This scheme uses homomorphic encryption Elliptic Curve Elgamal) algorithm to achieve data confidentiality and an homomorphic MAC algorithm based on message authentication code to achieve integrity of the data.

Secure End-to-End Data Aggregation in Wireless Sensor Networks [15] this paper represents a protocol for secure data aggregation, called secure end-to-end data aggregation, it provides end-to end data privacy of the aggregated data, the data is encrypted at sensor nodes and decrypted by the base station .This protocol uses additive homomorphic encryption technique for encryption of the data.

Secure Data Aggregation in Wireless Sensor Networks [16] this paper presents synopsis diffusion approach, this approach secure against the false data injection attacks in which malicious nodes inject wrong sub-aggregate values and a rare featherweight verification algorithm by which the base station can determine any wrong contribution in computed aggregate data.

Secure and Efficient Data Aggregation for Wireless Sensor Networks [17] presented the Leaf Node Representation Scheme (LNR) to solve ID problem in key stream-based encryption for WSN with static tree architecture, in this scheme leaf's node id can represent other node"s id in its route to the base station. The Delayed Hop-by-hop Authentication Scheme (DHA) guarantee the data integrity for WSN with dynamic cluster based architecture and it uses individual key for data encryption.

A New Approach to Secure Data Aggregation protocol for Wireless Sensor Networks [18] represented the approach which is based on revelation and clarification duplicitous sensor nodes with their sensed data. It uses outlier detection algorithm to find and clarify out the outlier sensor nodes. It provides high outlier revelation rate because to the use of distributed approach. It uses MAC for authentication of data and integrity of data. For providing confidentiality to data, symmetric encryption approach is used in this paper.

Table 1: Comparison of Security Protocols of Data Aggregation in WSN

Protocol	Architecture	Data confidentiality	Data Integrity	Data Authentication
TAG[7]	T	-	-	-
SIA[6]	T	+	+	+
SDRA[8]	G	+	-	-
SDAP[9]	T	+	+	+
SDAV[10]	T	+	+	+
SEDAN[11]	T	-	+	+
RSDA[12]	G	-	+	+
[13]	T	+	+	+
[14]	C	+	+	+

***Explanation of Symbols*:** T (Tree), C (Cluster), G (Grid), - (No), + (Yes)

4. Proposed Work

In this section, we will propose the algorithmic steps with the help of below data flow diagram: -

The following figure shows the DFD for proposed system. The network is divided by virtual rings. Next, the data is gathered by all the sensor nodes from their surrounding environment. Synopses and MACs are generated by the sensors. The synopses and respective MACs are then forwarded towards the BS ring by ring. The intermediate sensors perform the AND operation on the synopses accepted and their own synopses, later generate new MACs and forward them. The BS accepts the MACs and generates the data according to the MACs. If anomaly found, the BS calls for the MACs in the network and corrects the anomaly. The attacker node is removed from the network.

So, the flow diagram can be explained as follows: -
Input: Network, Base Station, Ring Topology
Output: A secure system
1. The sensors gather the data
2. For each sensor in network
3. Generate synopses for the data
4. If(sensor belongs to intermediate rings)

5. Accept the synopses from the outer ring sensors
6. Perform NAND operations with accepted synopses and generated synopses
7. End if
8. Generate MAC for synopses
9. Forward the Data and MAC to sensor in next ring
10. End for
11. If MAC request from BS
12. Forward MACs
13. End if
// at Base Station
14. Base station accepts the MACs from innermost sensors
15. Compare the MACs and received data
16. If anomaly detected
17. Send the MAC request to respective nodes
18. Accept the MACs
19. Correct the anomaly
20. Find and remove the attacker from network
21. End if
22. Generate the original Data.

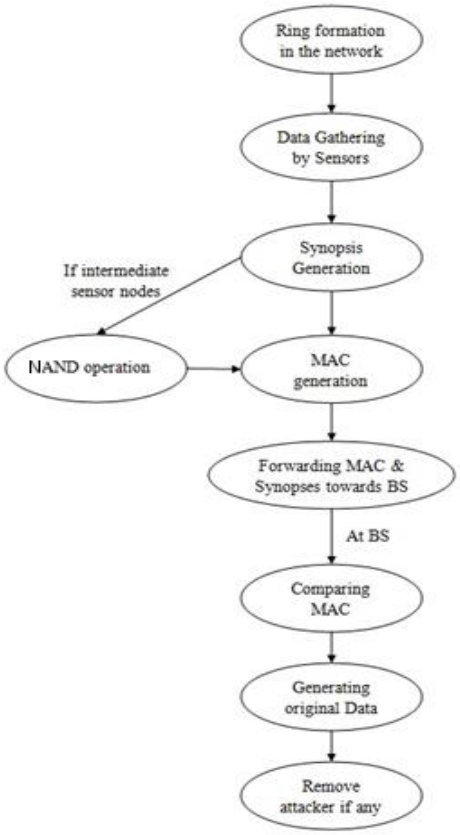

Figure 2: System Flow Diagram

5. Conclusion

Wireless Sensor Networks is very useful in various applications such as military surveillance, health, home, office monitoring and in many intelligent and smart systems. In Wireless Sensor Networks there are several issues to the security of the network and secure data aggregation is also a big issue. This report introduces a brief discussion of wireless sensor network, data aggregation, various approaches of data aggregation in WSN, Security needs to data aggregation, overview of various security protocols and their comparison.Firstly, the security issues of in-network aggregation algorithms to compute aggregates such as predicate Count and Sum were discussed. In particular, the falsified sub-aggregate attack launched by a few compromised nodes which can inject arbitrary amount of error in the base station,s estimate of the aggregate, were shown. An attack-resilient computation algorithm was explained so as to guarantee the successful computation of the aggregate even in the presence of the attack.

References

[1] Aashima Singla, Ratika Sachdeva "Review on Security Issues andAttacks in Wireless Sensor Networks",International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, 2013
[2] Vaibhav Pandey, AmarjeetKaur and Narottam Chand "A Review on Data Aggregation Techniques in Wireless Sensor Network", Journal of Electronic and Electrical Engineering Vol.1, Issue 2, 2010
[3] N.Sugandhi, D.Manivannan "Analysis of Various Deterioration Factors of Data Aggregation in Wireless Sensor Networks", International Journal of Engineering and Technology, ISSN: 0975-4024 Vol. 5 No 1 Feb-Mar 2013
[4] Kiran Maraiya, Kamal Kant, Nitin Gupta "Wireless Sensor Network: A Review on Data Aggregation",International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011
[5] Mukesh Kumar Jha, T.P Sharma "Secure Data aggregation in Wireless Sensor Network: A Survey", International Journal of Engineering Science and Technology, ISSN: 0975-5462, Vol. 3 No.3, March-2011
[6] B.Przydatek, D.Song, and A.Perrig"SIA: Secure Information Aggregation in Sensor Networks" in Proc. ACM conf.Embedded Network Sensor Systems, 2003
[7] S.Madden, M.J Franklin, and W.Hong "TAG: A Tinny Aggregation Service for Ad-Hoc Sensor Networks" in Proc. 5th Annual Symposium on Operating Systems Design and Implementation, Dec-2002
[8] S.Nath, P.B.Gibbons, S.Seshan, and Z.R.Anderson "Synopsis Diffusion for Robust Aggregation in Sensor Networks" in Proc. ACM conf. Embedded Network Sensor System Nov-2004
[9] Y.Yang, X.Wang, S.Zhu and G. Cao "A Secure Hop-by Hop Data Aggregation Protocol for Sensor Networks" in Proc. 7th ACM Int. Symp. Mobile Ad-hoc, 2006
[10] A.Mahimkar, T.S.Rappaport "A Secure Data Aggregation and verification Protocol for Sensor networks", IEEE Communications Society Globecom 2004
[11] M.Bagaa, N.Lasla, A. Ouadjaout, Y.Challal, "Secure and efficient protocol for Data Aggregation in wireless sensor networks", 32nd IEEE Conference on Local Computer Networks, 2007
[12] H.Alzaid, E.Foo, and J.G.Nieto "Reputation-based Secure Data Aggregation in Wireless sensor Networks" in Proc.1st int. Workshop on sensor Networks and Ambient Intelligence, 2008

[13] E.Mlaih, S.A.Aly "Secure Hop-by-Hop Aggregation of End-to-End Concealed Data in Wireless Sensor Networks"in IEEE international Conference, 2008
[14] S.B.Othman, A.Trad, and H.Youssef "Secure Data Aggregation with Mac Authentication in Wireless SensorNetworks", 12th Int. Conf. on Trust, Security and Privacy in Computing and Communications, 2013
[15] A.S.Poornima, B.B.Amberker "Secure End-to-End Data Aggregation in Wireless Sensor Networks", in IEEE international Conference, 2010
[16] S.Roy, M.Conti, S.Setia, and S.Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", in IEEE International Conference, 2012
[17] X.Wang, J.Li, X.Peng, and B.Zou "Secure and Efficient Data Aggregation for Wireless sensor Networks", in IEEE International Conference, 2010
[18] M.K.Jha, T.P Shrama, "A New Approach to Secure Data Aggregation protocol for Wireless Sensor Networks", International Journal on Computer Science and Engineering, vol. 2, No. 5, 2010
[19] H.Alzaid, E. Foo, J. G. Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey", Australasian Information Society Conference, vol. 81, Jan-2008
[20] P. D. Patel, P.B. Lapsiwala, R.V. Kshirsagar "Data Aggregation in Wireless Sensor Network", International Journal of Management, IT and Engineering, vol. 2, Issue 7 July-2012

Author Profile

Mr. Devendra S. Hapase, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. He received his B.E (Computer) Degree from SKNCOE, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is network security.