ISSN: 2321-8169
3746 - 3749

Robust Aggregation Mechanism in WSN for Mitigating Attacks

Jaber Ibrahim Naser
Department of Computer Science
Nizam College (Autonomous)
(A Constituent College, O.U)
Basheer Bagh, Hyderabad, India
abbas_jaber@yahoo.com

Mr. T. Ramdas Naik
Assistant Professor (B.E, Mca, M.Tech, Ph.D)
Department of IT Nizam College
Hyderabad, Telangana, India
ramdas_teja@gmail.com

Abstract--Wireless Sensor Network (WSN) is a collection of sensor nodes connected to base station which is characterized by many to one communication. Many sensor nodes will send data to base station making it many to on communication. The sensor nodes can act as sender and receiver of data as the data is sent to base station through intermediary nodes. The nodes are resource constrained as they are deployed in hostile environment or environment where resources are limited. The nodes are expected to participate in sensing or surveillance. WSNs are widely used in civilian and military applications for sending data and surveillance. As WSN is becoming increasingly popular, security needs to be provided in the network as the nodes are vulnerable to various attacks. Since the nodes are energy constrained, it is very useful to use some aggregation technique in order to reduce communication overhead and also energy consumption. Recently Roy et al. focused on aggregation in WSN for filtering out the impact of attackers on the network. Their focus was to use aggregation in WSN in order to reduce communication overhead and reduce the impact of attacks on WSN. In this paper we implement a variant of protocol that takes care of secure communications over WSN besides reducing energy consumption and mitigating attack impact. The simulation results are encouraging.

Index Terms *– Wireless Sensor Network, aggregation, energy efficiency, attack mitigation*

*****

I. INTRODUCTION

Wireless Sensor Network (WSN) is the network which is widely used in real world applications for monitoring and video surveillance [3], [2], [1]. Wireless sensor networks are energy constrained and thus they are vulnerable to various attacks such as Denial of Service (DoS), energy depletion attacks and so on. To overcome the security issues it is essential to have secure communications in such networks. A WSN can have plenty of sensr nodes which are able to send data to a sink node or base station. The base station holds the data sent by the sensor nodes. Sensor nodes can also act as router in order to send data through other sensor nodes. A typical WSN is as shown in Figure 1.

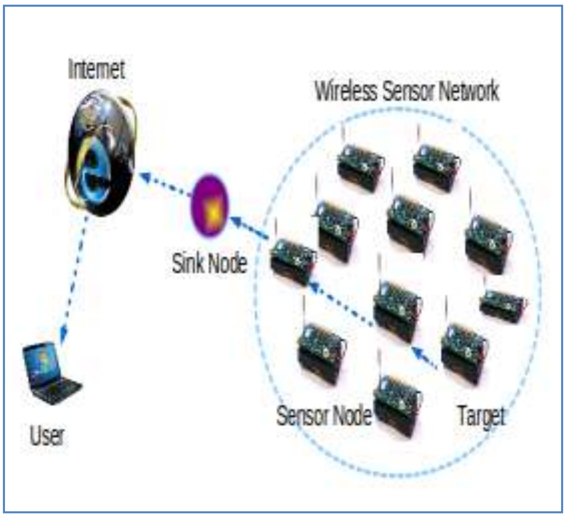

Fig. 1 – Typical wireless sensor network

As can be shown in Figure 1, wireless sensor network is a collection of sensor nodes which can sense data about targets. The sensor nodes sense the unknown object data and send to sink node. The sink node can be accessed by authorized users through Internet. In fact the sink node can be queried in order to monitor the area under coverage of WSN.

The sensor nodes can send data to base station through intermediary nodes. Thus each sensor node can act as receiver and sender of data. However, this kind of data transfer or communication is expensive and not energy efficient. Therefore in-network data aggregation [5], [6] scheme came into existence. The idea of this schme is to combine partial result at each node to enable efficient communication in WSN. The frequently used aggregates in the research community include SUM and COUNT. Recently Roy et al. [27] presented a synopsis diffusion approach that takes care of aggregation that will reduce the communication overhead besides reducing the probability of attacks or reducing the impact of attacks on WSN. In this paper we proposed a solution for data aggregation that can effectively mitigate the impact of attacks on the WSN. The remainder of the paper is structured as follows. Section 2 reviews literature on related works. Section 3 presents the proposed solution. Section 4 presents experimental results while section 5 concludes the paper besides giving recommendations for future work.

II. RELATED WORKS

This section provides review of literature on the data aggregation is Wireless Sensor Networks. Data aggregation routines include Count and Average in case of trusted environments as explored in [5]. Similar kind of work was proposed in [6]. In [14] another approach using tree based aggregation is used to achieve the same. However, there is communication loss problem in tree based models. In order to overcome this problem, in [8] a solution known synopsis diffusion was proposed. This technique makes use of ring topology in order to compute the Sum and Count aggregates. Similar kind of algorithms was also proposed in [7]. These solutions make use of duplicate-insensitive algorithm that is based on the [15] and its aggregate elements.

There were many other algorithms that came into existence [19]-[21]. However, they assumed that the base station is the only node that can have aggregate capabilities. However, in-network aggregation was not considered by these works. Recently there is much attention on the hierarchical aggregation. In [16] one such aggregation was proposed which was first of its kind and said to have resiliency against attacks. This scheme is said to be secure only in the presence of malicious nodes.

In [17] and [22] tree based verification algorithm was proposed and that has a BS that can detect final aggregate such as Count and Sum. The falsification attacks can be found in the process. There are other verification algorithms that made use of synopsis diffusion and computation of aggregates as explored [9] and [12]. Some novel protocols came into existence recently with the concept of secure outsourced aggregation [23]. There are some schemes [9], [17], [22] that do not allow base station from accepting false aggregates and there is not guarantee given for successful aggregate computation in the presence of attacks. Prior to the work of [12] synopsis diffusion framework that fails when there is attack. Another scheme known as SDAP [10] and with its attestation phase could compute Sum and Count aggregates even in the presence of multiple compromised nodes. Using Sum and Count, in [11] an algorithm is proposed which is DoS-resilent. Similar kind of research was done in [18] recently to prevent DoS attacks. The attack rsilent synopsis diffusion algorithm in [13] is more efficient. Resilient

III. PROPOSED SOLUTION

This section presents the proposed solution for data aggregation that can effectively mitigate the impact of attacks on the WSN. The aggregation of data is made using aggregates like SUM, COUNT and so on for the purpose of reducing communication overhead on the network. The aggregation also can help in improving efficiency in the network by reducing overall overhead on the network. Thus the proposed solution can benefit from the aggregation and improves network efficiency and supports secure communications as well. Since the transmission and node failures cause communication losses multi-cast routing is adapted in order to forward sub-aggregates.

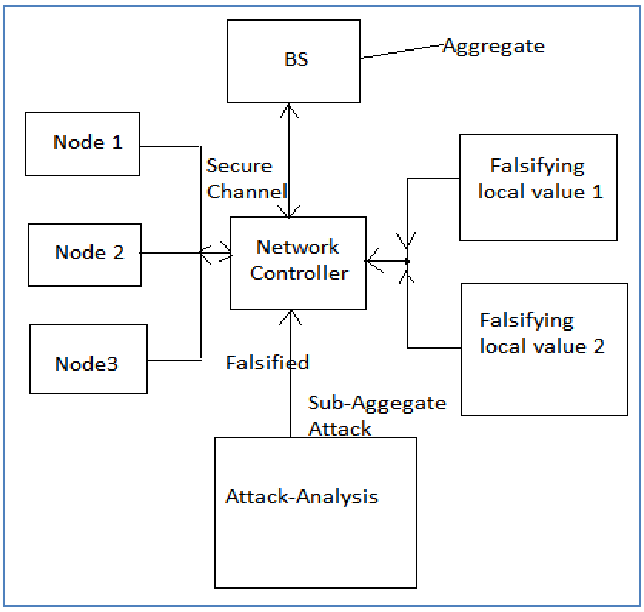

Figure 2 – Architectural Overview of the Proposed System

As shown in Figure 2, it is evident that the aggregation made through the routing nodes that are part of WSN. The data aggregation is the underlying feature of the network which ensures that the communications over it are secure and also the impact of attacks is minimized. There are components like base station, sensor nodes, network controller and attack-analysis node. The attack analysis module running in the network is responsible to filter out the data before being aggregated. The attacks made on the WSN nodes will be identified by analyzing the patterns and the attack related data is filtered out at the time of aggregation. This will potentially reduce the impact of attacks made on the network.

Compromise nodes in the network can launch falsified sub aggregate attack in order to deceive nodes and ensure successful attacks. The falsified sub aggregate attacks are tackled by the base station as it broadcasts an aggregate query and with a random value. The nodes in the network will answer the broad cast query along with MAC. Thus the base station is able to filter out malicious attacks while aggregating data. The potential attacks can be prevented thus using aggregation technique which will eventually mitigate the impact of attacks made on WSN. For any bit if the valid MAC address is not received, the base station identifies it as malicious and thus the impact of various attacks is reduced effectively.

IV. EXPERIMENTAL RESULTS

This section provides the environment used and the experiments and the results. The proposed system is implemented using Microsoft .NET platform. The application is the custom simulator that demonstrates the dynamics of a WSN. The proposed system is implemented using the architecture proposed in the previous section. The experiments are made in terms of number of compromised nodes vs. deviations of the estimate from r, number of compromised nodes vs. average per node sent bits, and number of compromised nodes vs. number of MACs.

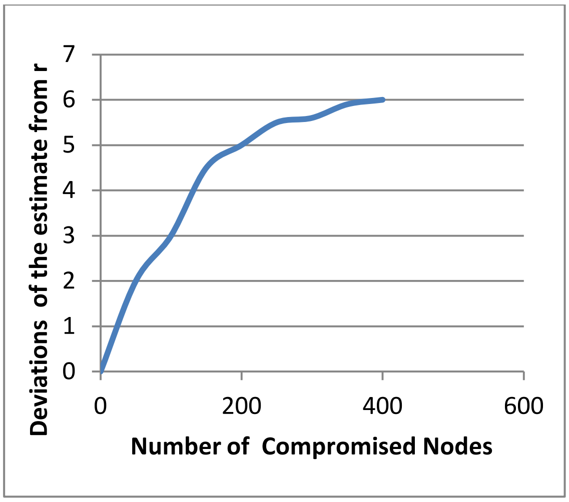

Figure 3 – Impact of number of compromised nodes

As shown in Figure 3, it is evident that the impact of the compromised node is more as the number of nodes is increased. When number of nodes is increased, the deviations of the estimate from r are more.

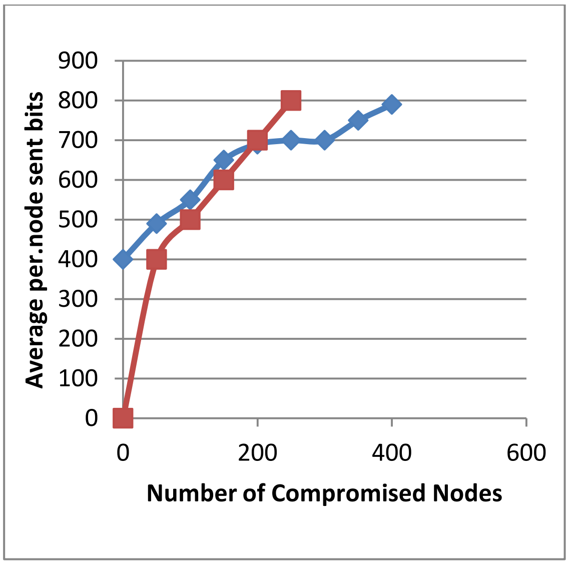

Figure 4 – Impact of number of compromised nodes

As shown in Figure 4, it is evident that the impact of the compromised node is more as the number of compromised nodes is increased. When number of nodes is increased, the average per node sent bits is more.

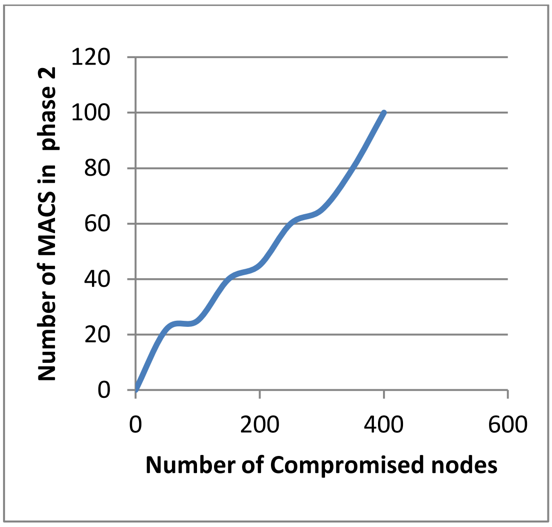

Figure 5 – Impact of number of compromised nodes

As shown in Figure 5, it is evident that the impact of the compromised node is more as the number of compromised nodes is increased. When number of nodes is increased, the number of MACs is more.

V. CONCLUSION AND FUTURE WORK

In this paper, we study the data aggregation techniques in order to use them in WSN for reducing possibility of attacks. In other words, data aggregation can mitigate the impact of attacks in WSN. The aggregation is the process of using aggregate functions like SUM, COUNT and so on in order to aggregate data which can reduce communication overhead besides reducing energy consumption. In this paper we proposed a variant for aggregation technique which focuses on making the mechanism more robust and thus mitigate the impact of attacks made on WSN. The simulation results reveal that the proposed approach is effective. Our future work includes exploration of more aggregate methods that can be used to exploit in order to reduce energy consumption and communication overhead further.

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] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, “Environmental wireless sensor networks,” *Proc. IEEE*, vol. 98, no. 11, pp. 1903–1917, Nov. 2010.

[4] (2006). *James Reserve Microclimate and Video Remote Sensing* [Online]. Available: http://research.cens.ucla.edu/ projects/2006/terrestrial/microclimate/defau%lt.htm

[5] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, "TAG: A tinym aggregation service for ad hoc sensor networks," in *Proc. 5th USENIX Symp. Operating Syst. Des. Implement.*, 2002, pp. 1–3.

[6] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring sensor networks," in *Proc. 2nd Int. Workshop Sensor Netw.Protocols Appl.*, 2003, pp. 139–158.

[7] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in *Proc. IEEE 20th Int. Conf. Data Eng. (ICDE)*, 2004, pp. 449–460.

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

[9] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-network aggregation," in *Proc. 23rd Int. Conf. Data Eng. (ICDE)*, 2007, pp. 996–1005.

[10] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A secure hop-byhop data aggregation protocol for sensor networks," in *Proc. ACM MOBIHOC*, 2006, pp. 356–367.

[11] H. Yu, "Secure and highly-available aggregation queries in large-scale sensor networks via set sampling," in *Proc. Int. Conf. Inf. Process. Sensor Netw.*, 2009, pp. 1–12.

[12] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7,no. 3, pp. 1040–1052, Jun. 2012.

[13] S. Roy, S. Setia, and S. Jajodia, "Attack-resilient hierarchical data aggregation in sensor networks," in *Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN)*, 2006, pp. 71–82.

[14] M. B. Greenwald and S. Khanna, "Power-conservative computation of order-statistics over sensor networks," in *Proc. 23th SIGMOD Principles Database Syst. (PODS)*, 2004, pp. 1–11.

[15] P. Flajolet and G. N. Martin, "Probabilistic counting algorithms for data base applications," *J. Comput. Syst. Sci.*, vol. 31, no. 2, pp. 182 -209,1985.

[16] L. Hu and D. Evans, "Secure aggregation for wireless networks," in *Proc. Workshop Security Assurance Ad Hoc Netw.*, 2003, pp. 384–391.

[17] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2006, pp. 278–287.

[18] B. Chen and H. Yu, "Secure aggregation with malicious node revocation in sensor networks," in *Proc. 31st Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2011, pp. 581–592.

[19] D. Wagner, "Resilient aggregation in sensor networks," in *Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN)*, 2004, pp. 68–79.

[20] L. Buttyan, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in *Proc. 2nd IEEE Workshop Sensor Netw. Syst. Pervasive Comput.*, Mar. 2006, pp. 331–336.

[21] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2003, pp. 255–265.

[22] K. Frikken and J. A. Dougherty, "An efficient integrity-preserving scheme for hierarchical sensor aggregation," in *Proc. 1st ACM Conf. Wireless Netw. Security (WiSec)*, 2008, pp. 68–76.

[23] S. Nath, H. Yu, and H. Chan, "Secure outsourced aggregation via oneway chains," in *Proc. 35th SIGMOD Int. Conf. Manag. Data*, 2009, pp. 31–44.

[24] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proc. Int. Conf. Mobile Comput. Netw. (MobiCOM)*, 2001, pp. 189–199.

[25] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. F. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks," in*Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 2045–2053 .

[26] S. Roy, M. Conti, S. Setia, and S. Jajodia. (2013). *Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. An Extended and Online Version* [Online]. Available: http://people.cis.ksu.edu/~sroy/attackResilientAgg.pdf

[27] Sankardas Roy,. (2014). Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. IEEE. 9 (4), p.499-502.

Authors:

JABER IBRAHIM NASER
DEPARTMENT OF COMPUTER SCIENCE
NIZAM COLLEGE (AUTONOMOUS)
(A Constituent College, O.U)
BASHEER BAGH, Hyderabad, India
abbas_jaber@yahoo.com

T. RAMDAS NAIK
Assistant professor (B.E, MCA, M.TECH, PH.D)
Department of it Nizam college
Hyderabad, Telangana, India
ramdas_teja@gmail.com