International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Analysis & Classification of Secure Data Aggregation in Wireless Sensor Networks

M Selvi, P M Joe Prathap

Abstract*: In several sensor functions, the data assembled from personage nodes is cumulative at a base station or host PC. To reduce energy exploitation, plentiful supports furthermore execute in-network aggregation of sensor data at transitional nodes reroute to the base station. The largest part accessible aggregation estimates and supports do prohibit any arrangements for security, and thusly these supports are powerless aligned with an extensive assortment of attacks. Exclusively, bargained nodes may be utilized to impart copied data that punctual inaccurate entire's being registered at the base station. We speak concerning the security vulnerabilities of data aggregation supports, and bring a study of powerful and secure aggregation protocols that are stretchy to false data concoction attacks.

Index Terms*: Data aggregation, Classification, Homomorphism and Secure Transmission.

I. INTRODUCTION

Wireless sensor networks (WSNs) picked up prominence in light of the way that they can be utilized to understand this present reality challenges with minimal effort [1-2]. WSNs are utilized in an assortment of uses, for example, living space observing [3] and target following [4] and so forth however these networks are obliged as far as assets, for example, memory, correspondence, calculation, and energy. WSNs comprise of an expansive amount of less energy and less power detecting gadgets known as nodes. Notwithstanding that are, there might live at least one influential gadget known as base stations. It manages the system and procedures the information gathered by the sensor nodes. These nodes sense and gather information from nature and propel it to the base station, which executes auxiliary inquiry on the gathered information. These nodes might live conveyed in region to one another since the quantity of nodes in the system might be substantial. Because of this region sensors might gather and broadcast repetitive information. While the broadcast of information expenses very huge than the calculation, it is generally worthwhile to compose these nodes in bunches. The information is prepared nearby inside the system and the totaled information is propelling to the base station in bunch condition. In this situation a few nodes what are known as the aggregators gather the information as of its nearby nodes progression it and propel the outcome to the base station. The system decreases correspondence separation and in this way energy utilization is lessened when contrasted with specifically correspondence by the base station. The situation is alluded to as information aggregation in prose.

Numerous protocols [5-8] encompass be planned for secure data aggregation in WSNs toward diminish the correspondence slide and the energy consumption. For the most part the system is isolated in to a hierarchy topology to be established on the base station. These nodes sense information as of the earth; the aggregators total the information as of the sensor nodes and propel the information to the base station. Construct position executes additional inquiry in light of the data.

Data aggregation decreases correspondence overhead essentially yet it constructs the security additional troublesome. Whichever bargain node may fashion information or may infuse wrong information in to the system and along these lines single traded off node may adjust the last aggregation [9]. As a rule the data aggregation lessens the correspondence transparency yet it releases novel ways to the enemy and also the totaled information may undoubtedly live harassed in the foe.

II. WSN DATA AGGREGATION

The design of the sensor network assumes critical job in the execution of information aggregation protocols. A few information aggregation protocols are be planned. This set of instruction may be grouped dependent on system representations. There are two types of classes: Tree based data aggregation [10] and group based data aggregation. Bunch based aggregations [11] are the way toward consolidating the information originating from different resources and in transit that in the wake of evacuating repetition, for example, to enhance the general system life span. The in-system handling is completed on the aggregator node.

The node aggregator total the information got as of its youngster node according to the requisite aggregation work (like low, high, normal, entirety and so forth.) and transmit the amassed outcome to the next abnormal state collected node. An Aggregation circumstances utilizing come together appeared in Figure 1 in so as to bunch craniums gather the information from every one of the nearby sensor nodes and sent that information to the Base Station. It again transmits that information to the outside system by means of Internet.

Manuscript published on 30 April 2019.
* Correspondence Author (s)
M Selvi, Research Scholar, Sathyabama Institute of Science and Technology, Chennai, India.
P M Joe Prathap, Associate Professor, Department of Information Technology, RMD Engineering College, Chennai, India.

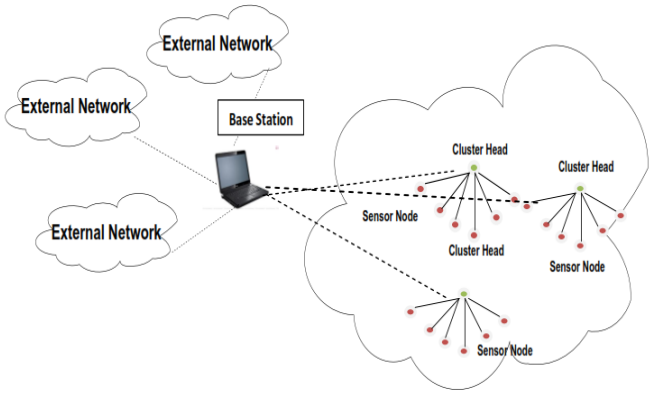

Fig.1 Clustering used WSN Data Aggregation Scenario

III. SECURE DATA AGGREGATION CLASSIFICATION

The effort on secure data aggregation may be arranged dependent on encryption of information at particular nodes divided by some classifications, jump by-bounce scrambled information aggregation back-to-back encoded information aggregation [12] and seclusion homomorphism.

A. Data Aggregation Encrypted by Hop-by-Hop: In the hop-by-hop scrambled information aggregation [12], transitional nodes decode each communication gotten through that. Along these lines, acquire the plain text .Then total the plaintext as per the total capacity, as well as encode the total outcome prior to conveying it. In this, every center of the road sensor node needs to unscramble the gotten information and relate aggregation work by it. Because of numerous decoding execute on the middle node its expending extra sequence power and won't give end-to-end protection.

B. Data Aggregation Encrypted by End-to-End: With the end goal to conquer the disadvantages of the jump by-bounce encoded data aggregation [13] an understanding of end-to-end twisted data aggregation protocols are anticipated. In those tactics, middle of the road nodes may entirety the form message uncomplicatedly lacking unscrambling the communication. Compared by the bounce by-jump solitary, it may ensure the conclusion to-end data solitude and consequence in fewer communication inactivity and computation rate. Foes won't encompass the capability to distinguish what considerate it is among data transmission. Concerning privacy, they intended means to dispense with surplus checking for data conglomerating though this examining resides anonymity to the aggregator.

C. Privacy Homomorphism: This [14] is an encryption change so as to permits coordinate calculation on scrambled information. In homomorphism encryption convinced aggregation capacities may be ascertained by the encoded information. The information is encoded and propels to the base station, even as sensors next to the way relate the aggregation work by the scrambled information. The base station gets the scrambled total outcome also it decodes. In particular, a homomorphism encryption plot enables the accompanying possessions to seize.

$$enc\ (a + b) = enc\ (a) + enc\ (b)$$

It implies with the end goal to compute the SUM of two qualities, we preserve concern a few capacity to their encoded partners also after that decode the consequence of the SUM activity on sink node. The information must be encoded in the sensor node, the AVERAGE or SUM MUST be computed since the total outcome pursues a way by the base station, also the last outcome must be unscrambled in the base station.

IV. METHODS AND DISCUSSION

The mixes of detached, dynamic and corporeal bothers by scholarly foe consequences in node detain harass [15]. The enemy introduces assail in social occasion the information's concerning WSN in catching impressive on communication trades. It is executed moreover nearby to lone antagonistic gadget or through whole system through the assistance of a few ill-disposed gadgets sorted out in the whole network. Alongside uninvolved taking in, the foe progressively participates in system protocols, asking the system with respect to the data also infusing noxious data in the system. The foe plays out the corporeal assaults, subsequent dynamic and aloof erudition. To improve the capacity of the assault identified with confident assault purpose, the accumulated data may be used to help the foe in picking the sensor node [16]. There are two sorts of node imprisons conceivable:

- Casual node imprison
- Discerning node imprison

The above node imprisons shifts in the type conveyance data to the aggressor. The aggressor must least detain many sensor nodes amid choosy node imprison assaults [17].

Issue Detection: In sensor node trade off strategy, there is an inception of node imprisons assault somewhere the foe actually imprisons the sensor nodes, expels that, and bargains also redistributes that in the system. Subsequent the redistribution of the traded off nodes, this develops an assortment of assaults during bargained nodes. The mighty invader debilitates the sensor system protocols alongside the arrangement of groups, steering, and data aggregation also consequently bringing about intermittent interruption of network activities. In this manner, the node imprison assaults are perilous and should be recognized at the earliest opportunity for diminishing the harms caused by them [18]. Amid the node imprison assaults, the enemy endeavors to alter the node actually to separate the insider facts of the cryptography. In view of the sanctuary engineering of the system, this sort of assault is profoundly dangerous and besides effects in compelling insider attacks.

A security concern of WSN compares to node imprisons assault by prompts trade off in the correspondence of an entire sensor system. In this protocol, the confirmation and sanctuary to keep up the effectiveness of the data aggregation is fused. At whatever point a sensor node needs to transmit information to a different node; initially the sensor node scrambles the information utilizing a solution and propels it to the aggregator. On behalf of respectability of the information bundle, a MAC depends confirmation system is utilized.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The security issue of WSN, for example, node imprison assaults isn't contemplated. This node detain assault is hurtful for system correspondence in system information aggregation, directing etcetera.

V. PERFORMANCE ANALYSIS & RESULTS

An alternate system parameter investigation is being improved the situation the proposed and existing protocols. Parameters like aggregate vitality utilization, throughput, packet conveyance proportion and deferral are looked at for the proposed and the current protocols.

Delay: It is characterized as the normal time taken by the packet to achieve the server node from the customer node. The routing protocol should create certain that the delay practiced by the data packets in the ad hoc network is smallest amount and an excellent performance is guaranteed always.

Delay = Number of transmitted packets / Time taken for Simulation

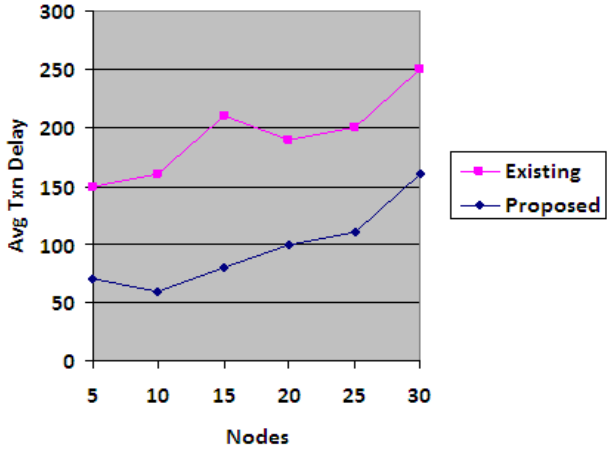

Fig.2 Performance of delay

Delivery Ratio: Packet Delivery Ratio is characterized as the normal of the proportion of the quantity of information packets got by every recipient over the quantity of information packets sent by the source.

Delivery ratio = Number of received packets / Number of transmitted packets

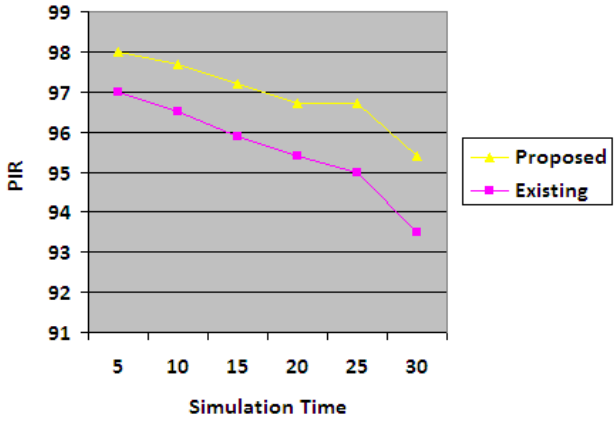

Fig.3 Performance of packet delivery ratio

Throughput: Throughput is the quantity of helpful bits per unit of time sent by the system from a specific source deliver to a specific goal, barring protocol overhead, and barring retransmitted information packets.

Throughput = Number of Received Packets / Time taken for Simulation

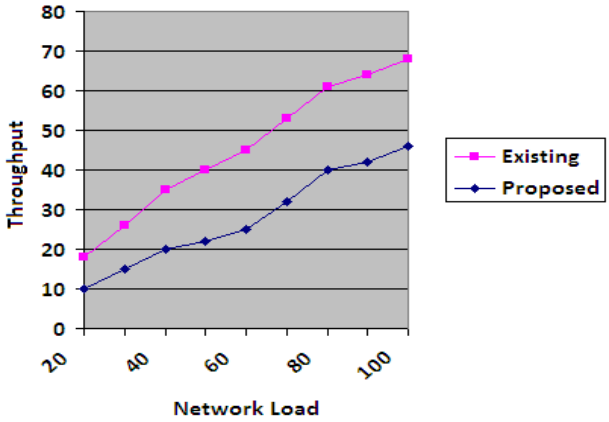

Fig.4 Performance of throughput

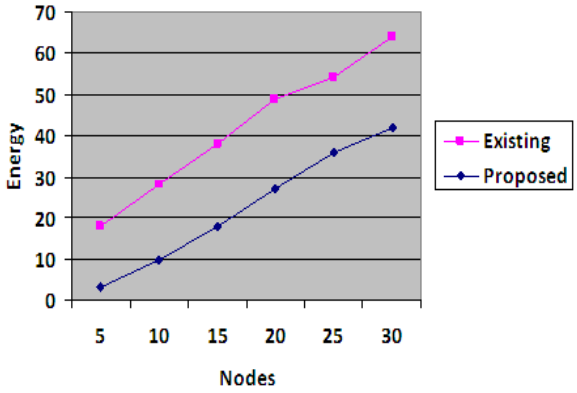

Fig.5 Performance of energy consumption

VI. CONCLUSION

In this paper, we have discussed about the security vulnerabilities of data aggregation protocols for sensor networks. We additionally displayed an overview of secure and versatile aggregation protocols for both single-aggregator and various leveled frameworks. Various difficulties stay in the region of secure aggregation for sensor net-works. Secure tree-based aggregation protocols stay defenseless against message misfortunes either because of node disappointment or traded off nodes. The execution and security tradeoffs between strong tree-based methodologies and multi-way methodologies, for example, Attack Resilient Synopsis Diffusion presently can't seem to be investigated. The examination network is yet to plan a secure aggregation protocol for figuring all encompassing totals, for example, Order-measurements and Most Frequent Items. At long last, numerous data procurement frameworks utilize industrious questions in which nodes intermittently send readings to the sink bringing about streams or flows of sensor data. These frameworks make broad utilization of data aggregation. Issues in anchoring such sensor data spilling applications stay to be researched.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

1. Sardaraz M, Tahir M, A A Ikram, “SDAF: A Secure Data Aggregation Framework for Wireless Sensor Networks”, Int. Jou. of Comp. and Elec. Engg., Volume 5, Issue 5, 2013, pp.447–450.
2. Akyildiz F, Su W, Sankarasubramaniam Y, Cavirci E, “A survey on sensor networks”, IEEE Comm. Mag., IEEE Computer Society, 2002, pp.102-114.
3. Mainwaring A, Polastre J, Szewczyk R, Culler D, Anderson J, “Wireless sensor networks for habitat monitoring”, in Proceedings of the 1st ACM Int. Workshop on WSNs and Applications, 2002, pp.88–97.
4. He T, Vicaire P, Yan T, Luo L, Gu L, Zhou G, Stoleru R, Cao Q, Stankovic A, Abdelzaher T, “Achieving real-time target tracking using wireless sensor networks”, in Proceedings of the 12th IEEE Real Time Technology and Applications Symposium, IEEE Computer Society, 2006, pp.37–48.
5. Intanagonwiwat C, Estrin D, Govindan R, Heidemann J, “Impact of network density on data aggregation in wireless sensor networks”, in Proceedings of the 22nd IEEE Int. Conf. on Distributed Computing Systems, IEEE Computer Society, 2002, pp.457–458.
6. Krishnamachari B, Estrin D, Wicker S, “The impact of data aggregation in wireless sensor networks”, in Proceedings of the 22nd IEEE Int. Conf. on Distributed Computing Systems, IEEE Computer Society, 2002, pp. 575–578.
7. Madden S, Franklin J, Hellerstein M, Hong W, “TAG: A tiny aggregation service for ad-hoc sensor networks”, in Proceedings of the 5th ACM Symposium on Operating Systems Design and Implementation, 2002, pp. 131-146.
8. Yang Y, Wang X, Zhu S, Cao G, “SDAP: A secure hop-by-hop data aggregation protocol for sensor networks”, in Proceedings of the 7th ACM Int. Sym. on Mobile Ad Hoc Networking and Computing, 2002, pp. 356–367.
9. Hu L, Evans D, “Secure aggregation for wireless network,” in Proceedings of the 2003 IEEE Symposium on Applications and the Internet Workshops, IEEE Computer Society, 2003, pp. 384–394.
10. Fasolo E, Rossi M, “Network Aggregation Techniques For Wireless Sensor Networks: A Survey”, IEEE Wireless Communications, Vol. 14, Iss. 2, 2007, pp.70-87.
11. Mukesh K J, T P Sharma, “Secure Data aggregation in Wireless Sensor Network: A Survey”, Int. Jou. of Engineering Science and Technology, Vol. 3, No. 3, 2011, pp.2013-2019.
12. Pambhar V, Bangoria B, Kataria B, “A Framework: Secure Data Aggregation in Wireless Sensor Networks”, Int. Jou. of Advanced Research in Electri., Electro. and Instru. Engg., Volume 2, Iss. 7, 2013, pp.3077-3082.
13. D Westhoff, J Girao, M Acharya, “Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution and Routing Adaptation”, IEEE Transactions on Mobile Computing, Volume 5, Issue 10, 2006, pp.1417-1431.
14. Ferrer J D I, “A new privacy homomorphism and applications”, Information Processing Letters, 60[5], 1996, pp. 277–282.
15. Bhoopathy V, Parvathi R M S, “Secure Authentication Technique for Data Aggregation in Wireless Sensor Networks”, Jou. of Computer Science, Volume 8, Issue 2, 2012, pp.232-238.
16. P Tague, R Poovendran, “Modeling node capture attacks in wireless sensor networks”, Proc. of the 46th Annual Allerton Conf. on Comm., Control and Computing, IEEE Explore Press, 2008, pp.1221-1224.
17. K Ren, W Lou, Y Zhang, “LEDS: Providing location-aware end-to-end data security in wireless sensor networks”, IEEE Trans. Mobile Comput., Volume 7, 2008, pp.585-598.
18. J W Ho, “Distributed detection of node capture attacks in wireless sensor networks”, Smart Wireless Sensor Networks, In Tech Publisher, ISBN 978-953-307-261-6, 2010, pp.345-360.