ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Survey on Energy Efficient & Secured Data Routing in Wireless Sensor Network

Rutuja Ashtikar, Prof. Deepali Javale

ME 2nd year Student, Department of Computer Engineering, MITCOE, Pune, University of Pune, India

Asst. Professor, Department of Computer Engineering, MITCOE, Pune, University of Pune, India

ABSTRACT: In recent years, wireless sensor networks (WSNs) become a major and challenging technology for the sensing of information in different application areas. There are various challenges in WSN, among which secure data routing is most difficult to resolve in network. This happens because of the way of node deployment in unattended or even hostile environments. The important metrics of routings are robustness, energy preservation, network lifetime etc. Security is also a major concern of data routing. In this paper, we focused on the various techniques that provide the security solution in data routing in presence of various attacks. This paper also investigates some latest approaches for secure data aggregation in WSN. Finally discuss the research gap in this area. We also provide the comparative analysis of such approaches based on their advantages and disadvantages.

KEYWORDS: Data aggregation, data routing, collusion attacks, wireless sensor networks

I. INTRODUCTION

A Wireless sensor networks (WSNs) are becoming progressively popular in numerous circles of life. Application areas include monitoring of the environment such as temperature, humidity and seismic activity as well as numerous other ecological, law enforcement and military settings to carefully pass their information through the network to a primary location. In the meantime, WSNs are regularly conveyed in public or generally un-trusted and even unfriendly situations, which prompt various security issues. These incorporate the usual topics, e.g., key administration, security, access control, authentication and DoS resistance, among others.

The sensor network faces the issue in changing or energizes the node batteries because of dense and ad-hoc operation in dangerous environment and due to unattended nature of WSNs. The critical question arise is how to increase the network lifetime of the sensor networks. Increasing the lifetime of the system through reducing the energy is a challenging issue in WSNs. Exploratory estimations have demonstrated that for the most part information transmission is extremely costly regarding in terms of energy consumption (EC), while information processing consumes appreciably less. Consequently, a practical approach to increase the WSN lifetime is to decrease the sensor energy consumption in data transmissions. Second problem face in the wireless sensor network is the security of data while sending the data from source to destination.

When sensor nodes with constrained resources can be subject to numerous types of attacks, the information encryptions are essential in WSNs. If encryption plan is not utilized, attackers can examine and introduce false information into the system. In hop- by- hop encoded data aggregation (EDAs), which is an intermediate aggregator possessing keys of all related sensor nodes decodes received encoded values, totals all the decoded values, and encodes the outcome for broadcasting to a base station (BS). This methodology requires that intermediate aggregators store keys for decryption in which a captured aggregator would uncover these secret data.

The WSN basically faces three challenges. First is increasing the network lifetime of the sensor network by minimizing the energy consumption in the network. Second is to provide the security while the data transmission from sender to receiver node or from sender to base station. Third is data loss recovery, while sending the data to the base station or cluster head data is loss, hence there is need to recover the data. In this paper we will see some of the work performed by the researchers on the WSN to solve the problems of secure data routing in WSN.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

II. RELATED WORK

In this paper [1], author presents an attacks which known as collusion attack other than existing IF algorithms. Furthermore an advancement in the IF algorithms is offered to oversee as of late displayed collusion attack. An underlying estimate of the consistency of mobile nodes gave advancement and the computation gets the chance to be collusion robust, precise and quicker converging. Constraint of this approach is not securing against traded off aggregator nodes. Author endeavoured to execute an approach in a deployed sensor network.

In this paper [2], the author studied their habitat, exhibit complex variability in shape and appearance; perform rapid motions against dynamic backgrounds with rapid illumination changes. They describe three applications that exemplify these problems and the solutions they developed. First, they show how temporal over-sampling can simplify the analysis of a slow process such as the avian nesting cycle. Then, we show how to overcome temporal under-sampling in order to detect birds at a feeder Station. Finally, they show how to exploit temporal consistency to reliably detect pollinators as they visit flowers in the field.

In this paper [3], the author demonstrated that Remote sensor systems are frequently questioned for totals for example, predicate number, aggregate, and normal. In untrusted situations, sensors might possibly be traded off. Existing approaches for safely noting conglomeration inquiries in untrusted sensor systems can distinguish whether the accumulation result is undermined by an assailant. Be that as it May, the assailant (controlling the traded off sensors) can continue defiling the outcome, rendering the framework inaccessible. This paper intends to empower accumulation inquiries to endure rather than simply recognizing the enemy. To this end, they propose a novel tree testing calculation that straightforwardly uses examining to answer total inquiries. It influences a novel set examining strategy to defeat a key and understood hindrance in examining — conventional testing strategy is just successful when the predicate check or total is extensive. Set testing can productively test an arrangement of sensors together, and decide whether any sensor in the set fulfills the predicate (in any case, not what number of). With set inspecting as a building square, tree inspecting can provably produce a right reply regardless of antagonistic obstruction, while without the disadvantages of customary testing method.

Hop by hop information total is an imperative strategy for decreasing the correspondence overhead and vitality use of sensor hubs amid the procedure of information accumulation in a sensor system. Be that as it may, in light of the fact that individual sensor readings are lost in the per hop total procedure, traded off hubs in the system might fashion false values as the total consequences of different hubs, deceiving the base station into tolerating spurious accumulation results. Here a principal test is: by what means can the base station acquire a decent guess of the combination result when a small amount of sensor hubs are traded off? To answer this test, author proposes SDAP, a Secure Hop-by hop Information Aggregation Protocol for sensor systems. The outline of SDAP depends on the standards of gap and-overcome and commits and-bear witness to. To begin with, SDAP utilizes a novel probabilistic gathering strategy to powerfully parcel the hubs in a tree topology into different coherent gatherings (sub trees) of comparable sizes. A commitment based jump by-bounce total is performed in every gathering to produce a gathering total. The base station then distinguishes the suspicious gatherings taking into account the arrangement of gathering totals. At last, each bunch under suspect takes part in a verification procedure to demonstrate the rightness of its gathering total. Our investigation and reproductions demonstrate that SDAP can accomplish the level of proficiency near a common jump by-bounce collection convention while giving certain affirmation on the reliability of the total result. Besides, SDAP is a broadly useful secure total convention material to different total capacities [4].

In [5] authors presented secure in-network aggregation algorithms for wireless sensor networks considering the possibility that a fraction of nodes might become compromised. In particular, we designed verification algorithms and attack-resilient computation algorithms to compute basic aggregates, such as Count, Sum and Median. Using a verification algorithm, the base station can verify the correctness of the computed aggregate, while an attack-resilient computation algorithm guarantees the successful computation of the aggregate despite the presence of attacks.

In paper [6] author proposed special end-to-end acknowledgment-based method, named EACK, for reliable data collection in WSNs is developed. Contrary to existing methods, the EACK resists collusion black hole attacks without using public-key cryptography, independent of MAC layer protocol, and does not need node-disjoint paths.

In paper [7], authors proposed improved iterative filtering technique. Proposed system is specially designed for both security and QOS which include insecure data aggregation mechanism, data validation of sensors Iteration Filtering algorithm. If any false data are detected, which node sends that data that node will be eliminated by a network also compression mechanism will improve the QOS of the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

To solve the secure localization problems in paper [8] authors developed a collusion attack model known as Collaborative Collusion Attack Model (CCAM) and propose a system Two-Step Format Detection (TSFD) system which is suited to WSN which is a resource constrained environment. The TSFD has reasonable and acceptable communication cost and algorithm complexity.

In paper [9] developed a game-theoretical model to detect intrusions and leading to a defense strategy for the WSNs. Authors given repeated game theoretical model to periodically punish a malicious node, and try to exploit the malicious node in favour of improving overall throughput of wireless sensor network.

In paper [10] authors have a secure and efficient range query protocol secRQ that can resist collusion attacks and probability attacks in tiered WSNs. secRQ preserves data privacy, enables storage nodes to process range queries precisely and supports the sink to defend against compromised storage nodes even if the network faces collusion attacks and probability attacks. Besides, we propose mutual verification scheme to verify the validity of query results. Thorough analysis and simulation results confirm the high performance of secRQ in terms of privacy preservation, integrity detection, efficiency and accuracy.

Table 1. Survey Table

Sr. No	Title	Method Used	Advantages	Disadvantages
1.	Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks	IF algorithms	Security is considered	protect against compromised aggregators
2.	Synopsis Diffusion for Robust Aggregation in Sensor Networks	Tree topology is used	Energy improvement, accuracy, Reliable	Double-counting sensor readings are done.
3.	Secure and highly-available aggregation queries in large-scale sensor networks via set sampling	tree sampling directly uses sampling	can potentially be applied to other problems	Efficiency can be increased
4.	EACK: End-to-End Acknowledgement-Based Method for Reliable Data Collection in Wireless Sensor Networks	public-key cryptography, independent of MAC layer protocol	decreases the network overhead and increases the packet delivery ratio	---
5.	A profile based scheme for security in clustered wireless sensor networks	data validation of sensors Iteration Filtering algorithm	more accurate and faster converging	No mechanism provided for overhead minimization on the system

III. PROPOSED SYSTEM

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

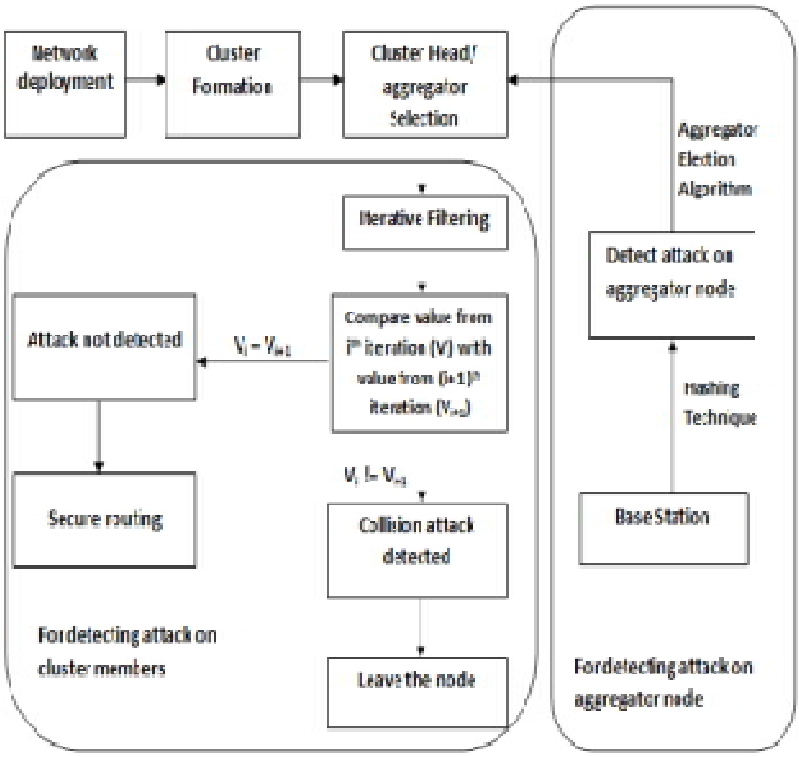

Fig 1. Propose System

IV. CONCLUSION

In this survey we have studied some of the work done by the researchers on the Wireless Sensor Network in details, also listed their advantages and disadvantages. This system presents some techniques that successfully resolve the problem of collusion attacks during data routing in WSN. By this study we can conclude that there must be a system which will solve the mentioned issues in the WSN to prolong the network lifetime and to reduce the energy consumption.

REFERENCES

1. M. Rezvani, A.rIgnjatovic, E. Bertino, and S. Jha, “Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks ”, IEEE transactions on dependable and secure computing, vol. 12, no. 1, january/February 2015.
2. 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. 250–262H. Yu, “Secure and highly-available aggregation queries in large-scalesensor networks via set sampling,” in Proc. Int. Conf. Inf. Process.SensorNetw., 2009, pp. 1–12.
3. H. Yu, “Secure and highly-available aggregation queries in large-scalesensor networks via set sampling,” in Proc. Int. Conf. Inf. Process.SensorNetw., 2009, pp. 1–12.
4. Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: A secure hop-byhop data aggregation protocol for sensor networks,” in Proc. ACMMOBIHOC, 2006, pp. 356–367.
5. 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,J,2012
6. V. Heydari and S. M. Yoo, "EACK: End-to-End Acknowledgement-Based Method for Reliable Data Collection in Wireless Sensor Networks," Information Science and Security (ICISS), 2015 2nd International Conference on, Seoul, 2015, pp. 1-4.
7. E. Brumancia and A. Sylvia, "A profile based scheme for security in clustered wireless sensor networks," Communications and Signal Processing (ICCSP), 2015 International Conference on, Melmaruvathur, 2015, pp. 0823-0827.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

8. J. Jiang, G. Han, L. Shu, H. C. Chao and S. Nishio, "A novel secure localization scheme against collaborative collusion in wireless sensor networks," 2011 7th International Wireless Communications and Mobile Computing Conference, Istanbul, 2011, pp. 308-313.
9. M. Estiri and A. Khademzadeh, "A game-theoretical model for intrusion detection in wireless sensor networks," Electrical and Computer Engineering (CCECE), 2010 23rd Canadian Conference on, Calgary, AB, 2010, pp. 1-5.
10. L. Dong, X. Chen, J. Zhu, H. Chen, K. Wang and C. Li, "A Secure Collusion-Aware and Probability-Aware Range Query Processing in Tiered Sensor Networks," Reliable Distributed Systems (SRDS), 2015 IEEE 34th Symposium on, Montreal, QC, 2015, pp. 110-119.