iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** I **Month of publication:** January 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Survey On Secure Routing In Wireless Sensor Networks

Meghana Shinde[1], Prof. Deepak Mehetre[2]
KJCOERM, Savitribai Phule Pune University,Pune, India

Abstract: ***In future, it is likely that wireless sensor networks (WSNs) become a major technology for the sensing in different application domains. The secure routing of data through the network is one of the main challenges in WSNs. This is resulting from the fact that WSNs are normally arranged in unattended or even hostile surroundings. While in last few years the routing approaches were mainly cynosure on metrics like robustness, preserving of energy, etc., recently, different security solutions came to the fore that were taking also the security problems in WSNs into account. In this paper,different routing system for WSNs are investigated. Consistently, measures for secure routing, including cryptography, key establishment, trust & reputation and localized security are taken on priority which were proposed by researchers in this area. Based on these findings, future prospects are discussed and final conclusions will be drawn.***
Index Terms: Black hole attack, network lifetime, security, trust, wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks (WSNs) including of hundreds or even thousands of small devices each with sensing, processing, and communication capabilities to monitor the real-world environment. They are envisioned to play an vital role in a wide variety of areas ranging from critical military surveillance applications to forest fire controlling and building security monitoring in the near future . In these networks, a huge number of sensor nodes are arranged to monitor a vast field, where the operational conditions are most often hard or even hostile. However, the nodes in WSNs have major resource constraints due to their lack of processing power, limited memory and energy. Since these networks are usually deployed in remote places and capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high left unattended, they should be completed with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead aren't feasible for resource constrained sensor nodes. The researchers in WSN security have proposed various security schemes which are developed for these networks with resource constraints. A number of protected and efficient routing protocols secure data aggregation protocols etc. has been proposed by several researchers in WSN security. In addition to traditional security problems like secure routing and secure data aggregation, security mechanisms deployed in WSNs also should involve collaborations among the nodes due to the decentralized nature of the networks and absence of any infrastructure. In live world WSNs, the nodes can not be assumed to be trustworthy apriori. Researchers have therefore, focused on building a sensor trust model to tackle the issues which are beyond the capabilities of traditional cryptographic mechanisms Since in most cases, the sensor nodes are unattended and physically insecure, vulnerability to physical attack is an vital issue in WSNs. A number of propositions exist in the literature for defense against physical attack on sensor nodes.

In WSNs one of the major research areas is the routing of data packets from a source to a destination through the network. Due to the finite energy resources, energy is one of the fundamental design requirements for routing protocols in WSNs. To store energy the transmission range of each sensor is critically limited so that data packets that should be transferred across the network have to be forwarded via multiple hops. Because of the topology changes, interferences caused by environmental influences or adversaries, node failures or perishing energy resources, the routing has to be failure-tolerant and has to accept permanently, while using as little energy as possible. With up-to-date routing data packets can be routed around critical areas so that a totally breakdown source and the destination. Moreover, the fusion of sensed of the network can be avoided. Therefore, the routing algorithm should take load balancing into account to avoid an overloading of certain nodes to decrease the exposure of partitioning the network, leading to missing paths among the

source and the destination. Moreover, the fusion of sensed data needs to be considered in WSN routing protocols to decreases redundant transmissions of the same data.

In communication unit, a common transceiver act as a communication unit and it is mainly used to transmit and receive the information among the nodes and base station and vice versa.

II. LITERATURE REVIEW

In paper authors have developed a sysem known as ActiveTrust. This system provides security against black holes via the active genration of a various detection routes for faster detectecion as well as getting nodal trust hence it maximize the security in data route. Also the creation as well as the distribution of detection routes are provided in the ActiveTrust that will utilize the energy in non-hotspots for creation of number of detection routes required for getting the needed security as well as energy efficiency

In paper authors have implemented a fully practical identity based encoded technique.given method has picked ciphertext security in the random oracle model reciving a modifyed computational Diffie-Hellman problem. Given system based on bilinear maps between clusters. The Weil mix on elliptic curve is a example of such a guide. They give a correct definition to secure identity based encryption schemes and give a couple of uses for such structures.

In paper authors have developed an security solution depending on the RAID5 technology as well as a multi-path routing, for implementing protective technique against the different attacks in mobile WSNs. Authors also have used this system on Probabilistic Routing Protocol by making use of History of Encounters and Transitivity (PRoPHET).

In paper authors have designed a secure routing technique that semirandomly sends a packet in the shortest path for the Sink by circumventing the faulty nodes. Various test runs demonstrated that the amount of broadcast hops,
network activity as well as the packet drop ratio are lesser for the developed routing method.

In paper authors developed a protocol based on weight known as AODV protocol, which is used for process of routing. In routing the weight of a route is given by four parameters those are nodes speed, level of power battery Bandwidth. The sensor nodes are devided in sevral clusters as well as a cluster head is selected in evry cluster. Communication in sensor as well as the sink takes place in the three levels as sensor to c1uster head to sink. Also a key management system for wireless sensor networks is utilized for reducing the memory as well as overhead on communication.

D Boneh and M. Franklin given a short mark plan in view of the Computational Diffie-Hellman supposition on certain elliptic and hyper-elliptic bends standard security parameters, the mark length is about a large portion of which of a DSA signature with a comparatory security level. Our short mark plan is intended for frameworks where marks are written in by a human or are sent over a low-transfer speed channel. They studied variety of properties of our mark plan, for example, signature total and clump check.

V. C. Gungor observed in paper , that Minimizing force utilization is urgent in battery force restricted secure remote portable systems. The author proposes following (a) demo an equipment setup/program to measure the battery power utilization to calculate encryption through genuine real-time experimentation, (b) to catch the connections between force utilization and security provide prowled information to propose scientific models, and (c) Prepare forms and gain security augmentation subject to power imperatives. Numerical results are introduced to measure the increase which can be achieved in utilizing arrangements of the proposed security boost issues subject to power requirements.

Table 1. Survey Table

Sr. No	Title	Year/Publication	Method Used	Advantages	Disadvantages
1.	ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks	IEEE, 2016	Data routing protocol	High energy efficiency	---
2.	Identity-based encryption from theWeil pairing	Springer,2001	Based on bilinear maps between groups and ciphertext security in the random oracle mode	Precised	---

3.	PRoPHET-RAIP5: A new approach to secure routing in wireless sensor networks	WINCOM, 2015	RAID5	Provides high level of security	end-to-end delay and energy consumption increase slightly
4.	Semi-randomised propagation for secure routing in Wireless Sensor Networks	ICRTIT, 2011	Point Propagation	Packet drop ratio are lesser	Can be extended to routing protocols
5.	Energy efficient secure routing in wireless sensor networks	ICETECT, 2011	Weight of the node	Improve the security of the network.	---
6.	Aggregate and verifiably encrypted signatures from bilinear maps	Springer,2003	Key generation, aggregation, and verification and Aggregate signatures and constructed an efficient aggregate signature scheme	Provide security	---

III. PROPOSED SYSTEM

An overview of the ActiveTrust scheme, which is composed of an active detection routing protocol and data routing protocol,

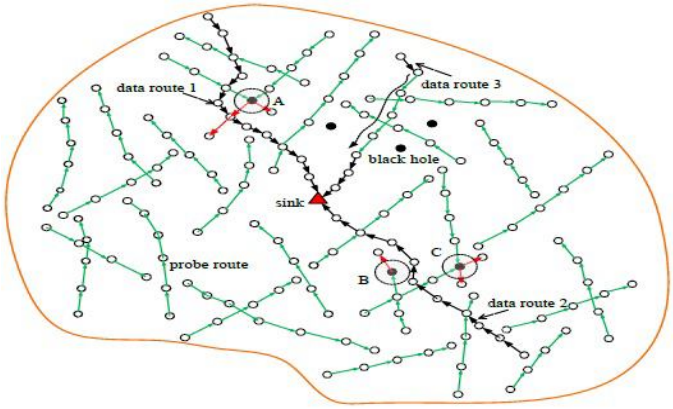


Fig. ActiveTrust Scheme

Security and trust routing through an active detection route protocol is proposed.

ActiveTrust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots.

Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security.

First, choose nodes with high trust to avoid potential attack, and then route along a successful detection route.

Through the above approach, the network security can be improved. System detect the Selective forwarding attack and make system more secure. Here in proposed network first source node select any one node from its neighbours. Then

check its distance from sink and trust. If trust is greater and distance is less then send information of packet size to that node otherwise select another node from neighbour list and check again trust is greater and distance is less then send information of

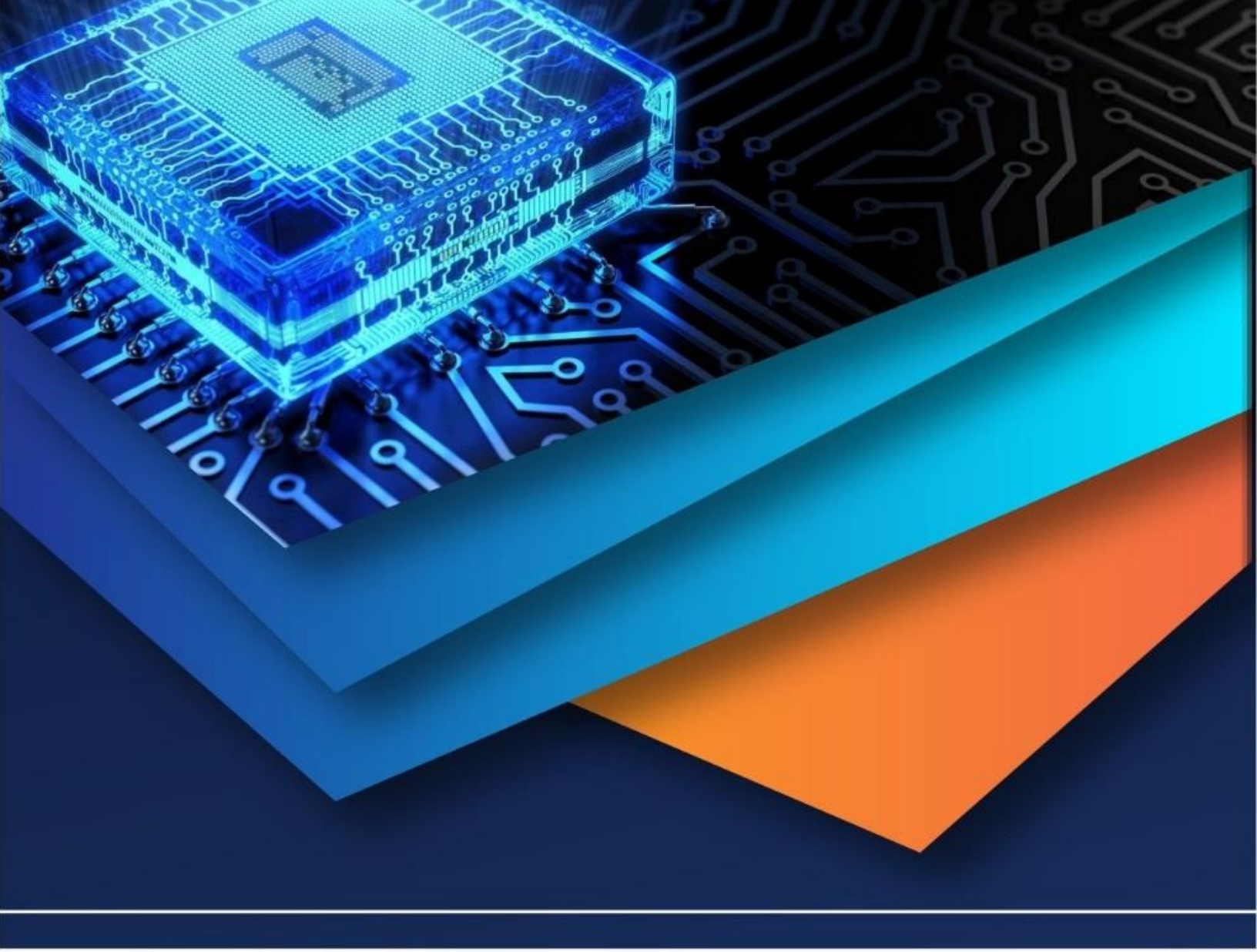
packet size to that node. This process continuous until path upto sink is detected. Each node checks size of data packet, if size of received packet is not equal to the size stored earlier then its previous node will send data to next node by discarding current node. If node and sink is same then data routed successfully otherwise again each node checks size of data packet, if size of received packet is not equal to the size stored earlier then its previous node will send data to next node by discarding current node.

IV. CONCLUSION

In this survey we have studied the some of the work done by the researchers on the topic of Secure Routing in Wireless Sensor Networks in details also listed some their advantages and disadvantages. By this study we can conclude that there must be a system which will solve the issues in the present systems.

REFERENCES

[1] Y. Liu, M. Dong, K. Ota and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013-2027, Sept. 2016.
[2] D. Boneh and M. Franklin, “Identity-based encryption from theWeil pairing”, SIAMJ. Comput., vol. 32, no. 3, pp. 586-615, 2003.
[3] R. E. Mezouary, A. Houmz, J. Jalil and M. E. Koutbi, "PRoPHET-RAIP5: A new approach to secure routing in wireless sensor networks," 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakech, 2015, pp. 1-6.
[4] S. P. T. Srinivasan and C. Chellappan, "Semi-randomised propagation for secure routing in Wireless Sensor Networks," 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, 2011, pp. 428-432.
[5] D. P. S. Edvinoe Christina and R. Jothi Chitra, "Energy efficient secure routing in wireless sensor networks," 2011 International Conference on Emerging Trends in Electrical and Computer Technology, Tamil Nadu, 2011, pp. 982-986.
[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encryptedsignatures from bilinear maps,” in Proc. 22nd Int. Conf. Theory Appl. Cryptograph.Techn., 2003, pp. 416-432.
[7] C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and challenges of wirelesssensor networks in smart grid,” IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557-3564, Oct. 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY