IJCSC 0973-7391 Volume 7 • Number 2 March 2016 - Sept 2016 pp. 213-217 available online at www.csjournalss.com

A Survey of Secure and Efficient Energy aware Routing for Spontaneous Wireless Sensor Network

Ms. Preeti Dixit, Dr. Vivek Sharma[1]
[1]Professor & Head (CSE)
Deptt. Computer Science and Engineering, T.I.T. Advance, R.G.P.V. University, Bhopal (M.P.)

Abstract: The absence of centralized administration is the main cause of attack in Wireless Sensor Network (WSN). The attacker presence is disorderly the appropriate communication in network through that the lot of useful data is drop or corrupted by attacker. Numerous numbers of attackers are present in WSN and each and every attacker is the different technique to do misbehavior in network. The nodes in WSN are performing power or energy constraint operations and each and every operation in WSN consumes energy and due to presence of attacker the lost of energy is wasted in retransmission and this energy source is in limited quantity available for each mobile nodes. The network topology are also not fixed the nodes in WSN are continuously moves and their movement is also one the reason of link breakage. The lost of researches are proposed the different security scheme to secure network from malicious nodes or attacker and proposed to do energy efficient routing to prolog network performance. The attacker is affected the network performance by dropping data packets and these packets are sender is try to retransmit. In this paper we present the survey of some previous techniques that are proposed by different researchers in field of energy and security. These researches are provides the many innovative works also motivate us to do something in innovative in field of energy efficient routing and secure routing.

Index Terms: Energy, Attack, Routing, Survey, WSN.

I. Introduction

A Wireless sensing element network include a large range of sensing element nodes that's accountable for industrial management and observation the atmosphere, new generation for commercial communication and every one the reading of sensing element nodes are collected by the base stations or sink nodes. Sensing element network embody numerous applications like military surveillance, sensing element nodes are deployed in large-scale, hostile environments within the network. The simplest example is that the use of sensing element networks for safety industrial applications and emergency scenario i.e. meteorology, earth information, environmental activity retrieval. This network might use sensors to find the presence of dangerous materials, and additionally provides the first detection techniques and identifies the leaks of chemicals or biological effects before extreme loss which may lead to public. The wireless networks uses the various routing protocol in distributed fashion, they need totally different path for routing, and may be maintained and healed by itself for more problems, they additionally resilient in an explosion or extreme inflicted loss to the industrial application, that provides public trust with important conditioned information within the hard constraints. The operations that are not processed due to systematically little sizes, sensing element nodes are continually at higher risk of being captured physically and having their compromised security within the network. The ability of sensing element nodes is not replaceable and also the nodes consist of less battery power. Reducing the energy consumption for information transmission and security for transmission the data through sensing element nodes are very essential in wireless sensing element network. If sensing element nodes area unit physically captured or compromised, vital lead like network keys or network number are often simply reveal to the attacker or adversary. Wireless sensing element network consist of range of network attacks that is not good for securely transmission of data over the virtual or physical network. therefore during this synopsis we have a tendency to focus to resolve the problem of security threats and resource management that is low energy utilization for the communication and supply reliable service to the end user in effective manner[4][5]. during this work we provide more secure communication using node capability based node trust estimation and energy aware based route establishment methodology, meanwhile observation node simply find the faulty node with low overhead and improve the network performance whereas attacker node present within the network.

II. Literature Survey

Wireless sensing element network are more vulnerable as compare to wired or wireless communication however in currently, number of analysis focus within the field of WSN, therefore in future the WSN is most utilized network in real application in every were. In this section we have a tendency to study range of latest papers beneath security and energy connected issue and its resolution in WSN field those are as follows.

Adnan Ahmed et. al. presented A Trust and Energy Aware Routing Protocol for Wireless sensing element Network (TERP) [1], during this paper, they gift a trust and energy aware routing protocol (TERP) that makes use of a distributed trust model for the detection and isolation of misbehaving and faulty nodes. Moreover, TERP incorporates a composite routing function that encompasses trust, residual-energy, and hop counts of neighbor nodes in creating routing selections. This multi-facet routing strategy helps to balance out energy consumption among trustworthy nodes, whereas routing

DOI: 10.090592/IJCSC.2016.134

information using shorter methods. Their simulation results demonstrate reduced energy consumption, improved throughout and network life of TERP when compared with the existing work.

Miss. Prachi S. Moon et. al. has an title on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless sensing element Network [2]. During this paper describes about the hybrid security techniques available for the intrusion detection and security. It additionally represented about the pros and cons connected with of these solutions. The secure hybrid mechanism provides an intrusion detection system beneath hybrid security algorithms to increase the level of security in wireless sensing element network for communication. Additionally it provides a positive performance against intrusion attack within the cases of less power transmission, receiver collision problem etc. this may be useful to users for secure data communication within the network. The hybrid mechanism is responsible for detection and interference of multiple attacks happens at same time at the same time, additionally it provides the strong encryption methodology for secure communication of data within wireless sensing element network.

Raja Waseem Anwar et. al. present a paper on title increased Trust Aware Routing against wormhole Attacks in Wireless sensing element Networks [3]. During this paper, they propose a trust aware distance vector routing protocol (T-AODV) to guard wireless sensing element network from wormhole attacks. Through experimental results, their propose approach tested the network potency in terms of improved packet delivery ratio, end-to-end delay and range of node to the destination.

Duan et al. presented a Trust-aware Secure Routing Framework (TSRF) [6] for WSN to counter node misbehaviour attacks. TSRF incorporates each direct and indirect trust for evaluating the trustworthiness of nodes. To avoid false recommendations from misbehaving nodes, an inconsistency check mechanism [7] is incorporated in TSRF’s trust model. Every node is initialized with neutral trust value. Afterwards, based on the evidences in packet forwarding the trust ratings are varied consequently. TSRF completely focuses on the identification of misbehaving nodes and circumventing them for the info transfer over multi-hop path. However, TSRF don't keep in read vital characteristics of WSN like energy and wireless interference that results in dead nodes and compromised network life. The procedure intensive mechanism incorporated for inconsistency check makes the trust convergence method slow and consumes vital resources. Moreover, TSRF don't optimize the end-to-end route choice and maintenance that consequently results in longer methods, high route instability and delays.

In [8], a trust based routing theme, friendship based AODV (Fr-AODV), is presented to counter blackhole attack. Trust analysis is based on certain options like node reputation and node identity. Each feature is assigned attribute range that is changed during packet forwarding. A source node asks its neighboring node to present its features’ attribute range. The source node verifies the attribute range, if the match is found, the neighbor node is granted to forward the packet. The node authentication is verified through the exchange of hello messages. However, the proposed answer isn't fully robust against node misconduct attacks. The authenticated compromised node might exchange false feature attribute range and its identity which can result in incorrect deciding by trust model. The increased range of route maintenance calls and exchange of hello messages increase routing overhead to vital level which can cause high energy consumption of trustworthy nodes.

To defend against wormhole attack in WSN, a trust aware routing framework (TARF) has been proposed [9]. A neighbor table is maintained by every node to keep record for trust and energy value values for legendary neighbors. Trust evaluation is based on detecting routing loops and nodes concerned in routing loops are penalized. Energy management messages are broadcasted that contains energy value data to deliver a packet. However, broadcasting of energy management packets might increase routing load and additionally it may suffer from selfishness attack wherever a compromised node may send false energy value data. A trustworthy node could also be declared as malicious node if it drops packets thanks to vital level of congestion. The effectiveness of proposed answer isn't evaluated in terms of consumed energy and network life that is a vital design parameter for WSN.

A Light Weight Trust based routing protocol (LTB-AODV) [10] is presented to defend against blackhole and grayhole attacks. LTB-AODV makes use of intrusion detection system (IDS) for trust estimation. The trust estimation is predicated on the packet forwarding behavior of the nodes. Every node is responsible for evaluating the express trust for its neighbor node. Additionally, it additionally incorporates indirect trust from neighbors. However, IDS based schemes exhibit certain vulnerabilities after they come back to handle insider attacks. The mobile nature of nodes builds it tough to differentiate traditional and abnormal traffic patterns and may make legitimate network traffic appear suspected [11]. LTB-AODV doesn't take into thought to balance load on trustworthy nodes particularly if a node has energy constraints that places a lot of burden on trustworthy nodes and will increase the likelihood of dead nodes thereby compromising route stability and network life. Moreover, thanks to uncontrolled range of route maintenance calls the routing overhead will increase to vital level.

Shiann Tsong Sheu, ming Tse Kao, Yen Hsu, Yen Cheng, [12] has proposed a secure routing methodology for sleuthing and preventing the network attack like false reports and Grayhole attacks in wireless sensing element networks. Throughout the analysis, it's found that a lot of the authors did not establish security threats and additionally to produce their measure to beat those explicit threats within the network. Their proposed method perfectly detects false report and Gray-Hole attack exploitation route filtering (SEF) theme. These proposed strategies additionally attempt to increase the extent of security considering each facet of the sensing element nodes within the

DOI: 10.090592/IJCSC.2016.134

network. It additionally reduces energy consumption by implementing Elliptical Curve Cryptography (ECC) for coding and secret writing method that provides a lot of security throughout information transmission.

Yassine maleha, abdellah ejati, [13] has conferred the techniques for security attacks in wireless networks, and major work is completed on comparison and analysis of recent Intrusion Detection schemes in wireless sensing element network. During this paper author has additionally introduces regarding the varied techniques for the detection of attack over each section of communication over the wireless sensing element network. This paper presents a review of the safety attacks in wireless sensing element network and analyzed a number of the prevailing Intrusion detection system models and architectures.

Seyedeh Yasaman Rashida, [14] has proposed a novel Intrusion Detection System exploitation Multi Agent theme in distributed wireless environment with the use of different sensing element nodes, for decreasing false alarms reports that are generated throughout transmission of data and manages misuse of knowledge and misuse of anomaly detection. During this paper two techniques are used relatively for anomaly detection like misuse signature-based detection and anomaly behavior primarily based detection. Main reason of applying each technique along is trying to find such reasonably network within the system for thriving secure communication over the network.

Dr. Harsh Kumar Verma, Saurabh Singh, [15] has represented about various problems associated with security attack that occur simultaneously within the wireless sensing element network at various layers of protocol design. This paper carries with it numerous constraints in wireless sensing element network, security availability and numerous varieties of network attack and their interference mechanism at totally different layers of protocol stack of wireless sensing element network has been presented consecutively. This paper presents a complete introduction regarding wireless sensing element networks, sensing element network communication design and numerous application of wireless sensing element network.

Md. Safiqul Islam, Syed Ashiqur Rahman, [16] has mentioned the different types of attacks on sensing element network and additionally prime emphasis is given on the anomaly primarily based intrusion detection system. They projected an IDS agent in every sensing element node and their IDS agent consists of native responses in network, Cooperative detection engine channel, local packet observation activities, and local detection devices in network. Native responses send the response packets to the bottom station if any anomaly is found. Throughout detection of attack by exploitation co-operative engine technique, data is shared with the opposite neighboring nodes to reduce the warning rates as per the intrusion is detected and prevented by any sensing element node.

Hichem chejelmachi, mohommad fahem, [17] has proposed a hybrid intrusion detection system for wireless sensing element network in clustered fashion. The author has proposed the methodology that uses a mixture of the Anomaly Detection supported support vector machine (SVM) and also the Misuse Detection method. This method involves the comparison between captured information and legendary attack signatures, specific pattern of knowledge packets are to be thought-about as an intrusion within the network. Intrusion detection is only targeted on analyzing the behavior of the nodes and their relatively captured information. With this detection model, any controlling activities that deviate from this model are often simply captured as an anomaly severally. The foremost advantage of such technique is that it will find attacks that don't seem to be revealed. Experiments results show that almost all of routing attacks are often detected and prevented with low warning that is appropriate in wireless sensing element network communication.

Jyoti Singhai, shweta Jainist, virendra pal Singh, [18] has proposed a method based on signal strength that has been used for detection and interference of hello flood attack in network. This paper shows the techniques for overcoming the matter of the flooding within the network specially communication from source to destination. Nodes are specifically classified into legendary nodes and unknown nodes, supported their signal strength mechanism that is comparatively used for the detection purpose. User which needs less power consumption and less battery power for communication and transmission is easily used to check the validity of affected nodes within the wireless sensing element network. This paper shows the safety framework for hello flood detection through signal strength and consumer methodology needs less power and energy for computation..

III. Proposed Work

Wireless sensor network (WSN) is a self-organized, low cost and composed with tiny communication and computing devices network used to monitor different environments. Typically sensor nodes deployment is very effective in harsh and hostile environment for cooperatively monitor and reports to sink node for further processing and analysis. The nature of wireless sensor network is liable to attack internally and externally. Malicious nodes launch security attacks in the network and lead to damage the different network functions such as routing, energy, channel utilization, etc [3]. For the different attack detection and prevention, we study number of latest research papers in the field of security and energy consumption, and those researches are to encourage towards the field of WSN reliability and resource management. In our proposed work we secure and efficiently utilized WSN resource based on node capacity, energy consumption and node monitoring based mechanism. For the fulfilment of proposed work very first we initiate the route request message and established the path from source to sink based on node capacity and energy requirement of per packet. Node capacity measure with the help of delay difference (packet incoming and outgoing from node that includes queue and processing delay) that helps to identifies data dropped reason (from attack or other network problem) and its helps to set threshold of node

DOI: 10.090592/IJCSC.2016.134

for reliability. Meanwhile energy consumption of node in per packet recognize from (nth packet time energy - nth - 1 packet time energy) and that energy consumption are useful for route establishment between source to sink. In the routing phase established path with low energy and node capacity based methodology. After that we random deploy monitor nodes in network, those nodes are monitor neighbour node activity and lightly detect attacker node, because node capacity module provide strength to monitoring node, for attacker working activity and its behaviour. While attacker node detected than re-route are established based on recursive procedure of our proposed work, but meantime previously detected attacker are eliminated from the network and increases the network reliability with low energy utilization. Above proposed approach is more secure and reliable with better quality of service against routing attack.

IV. Simulation Environment Overview

Network simulator 2 is the result of an on-going effort of research and development that is administrated by researchers at Berkeley. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols [19]. The simulator is written in C++ and a script language called OTcl2. Ns use an OTcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations.

A. Performance Evaluation

There are following different performance metrics have showed the results on the basis of following:

1) Packet delivery ratio:

The ratio of the data packets received at the destination nodes to the packets that were sent by the sources.

2) Routing load:

The number of routing packets (and supporting protocol control packets) transmitted per data packet delivered at the destination.

3) Throughput:

Throughput or network throughput is the average rate of successful message delivery over a communication channel from source to destination.

V. Conclusion:

WSN is a very sensitive network, because network topology dramatically changes time to time so every discrete time interval monitor and maintain route for reliable data delivery. Wireless sensor network is a form of un-trusted network and unstructured way of resource utilization so our aim to provide secure communication with low overhead and proper energy management based routing that improves the network performance. The number of nodes that communicate n network is continuously depleting their energy and this energy is utilized or waste depends on the number of packets receiving with respect to sending in dynamic network. The survey of different researches or work in field of security is able to secure the WSN from different attacks but most of them are focus on the detection of attack. The attacker malicious characteristics are the main detection and this detection is based on the attacker activation in network. The attacker is continuously perform malicious activities then in that case the proposed security scheme is able to detect and prevent it from network.

References

[1] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan, “TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network” IEEE Sensors Journal, Vol. 15, No. 12, December 2015.

[2] Miss. Prachi S. Moon, Mr. Piyush K. Ingole, “An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network” 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) MS Engineering College, Ghaziabad, India

[3] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi , “Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks” 2015 International Conference on Smart Sensors and Application (ICSSA), 978-1-4799-7364-4/15/2015 IEEE

[4] Shiann Tsong Sheu,Ming Tse Kao, Yen Hsu,Y en Cheng, “Secure routing protocol for detecting grayhole attack and false report along with elliptic curve cryptography in wireless sensor network” IEEE students conference on electrical, electronics and computer science 2014 IEEE.

[5] Somdip dey, asole nath, “MES-1 (modern encryption standard) an advanced cryptography method” IEEE 2012.

[6] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, “TSRF: A trust-aware secure routing framework in wireless sensor networks,” Int. J. Distrib. Sensor Netw., vol. 2014, pp. 1–14, Jan. 2014, Art. ID 209436.

[7] H. Deng, G. Jin, K. Sun, R. Xu, M. Lyell, and J. A. Luke, “Trust-aware in-network aggregation for wireless sensor networks,” in Proc. IEEE Global Telecommun. Conf. (GLOBECOM), Nov./Dec. 2009, pp. 1–8.

[8] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, “Trust-basedrouting mechanism in MANET: Design and implementation,” Mobile Netw. Appl., vol. 18, no. 5, pp. 666–677, Oct. 2013.

[9] G. Zhan, W. Shi, and J. Deng, “Design and implementation of TARF: A trust-aware routing framework for WSNs,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.

[10] N. Marchang and R. Datta, “Light-weight trust-based routing protocol for mobile ad hoc networks,” IET Inf. Security, vol. 6, no. 2, pp. 77–83, Jun. 2012.

[11] Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 275–283.

[12] Shiann Tsong Sheu,Ming Tse Kao, Yen Hsu,Y en Cheng, “Secure routing protocol for detecting grayhole attack and false report along with elliptic curve cryptography in wireless sensor

network" IEEE students conference on electrical, electronics and computer science 2014 IEEE.

[13] Yassine maleha,abdellah ejati, "A review of security attacks and intrusion detection schemes in wireless sensor networks," international conference on emerging trends in computer science and technology, july 2013.

[14] Seyedeh Yasaman Rashida, "hybrid architecture for distributed intrusion detection system in wireless sensor network" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013 IEEE.

[15] Dr. Harsh Kumar Verma, Saurabh Singh, "security for wireless sensor networks" International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011 IEEE.

[16] Md. Safiqul Islam, Syed AshiqurRahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches" International Journal of Advanced Science and Technology Vol. 36, November, 2011.

[17] Hichem chejelmachi, mohommad fahem, "Novel hybrid intrusion detection system for clustered wireless sensor network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011 IEEE.

[18] Jyoti Singhai,shweta jain, virendra pal singh, "Hello flood attack and its counter measures in wireless sensor networks" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[19] The Network Simulator – ns-2 http://www.isi.edu/nsnam/ns/