ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 12, June 2020

An Efficient security scheme of Detection and avoidance of Operational Malicious Node Flooding in Wireless Network

James Kiby, P S Alanzi

Abstract*—The energy efficient communication is very essential in network as charging batteries and node replacement in emergency conditions like floods, expected volcano eruptions is nearly impossible. In this paper, the security scheme against flooding attack to secure clustering based routing is explained. The selection of cluster head (CH) is based on higher residual energy and rest of the cluster members (CM) transfers information outside the cluster with the help of CH. There are separate CH and CM in each group. The performance of LEACH protocol is affected by flooding attackers. This paper security scheme identifies the attacker's malicious functions and blocks their presence. The performance of proposed protocol is compared with existing TESDA protocol. The TESDA protocol selects the maximum energy CH and whole communication security depends on trust value. The TESDA trust value depends on packets received at destination and flooding attacker blocks the available limited bandwidth. The proposed work provides the reliable routing scheme to improve network performance using minimum energy cost. The minimum energy consumption enhances the possibility of secure communication which in result enhances the network lifetime. The performance of proposed security scheme, TESDA and flooding attack is evaluated through performance matrices like PDR, energy consumption, overhead and delay.

***Keywords*:- Flooding attack, Security, LEACH, Energy, Routing, WSN.**

I. INTRODUCTION

WSN Wireless sensor Network can be a self-organizing, self-configuring and multi-hop wireless network that is a dynamic kind of a network wherever nodes will communicate with one another with none existing network infrastructure like access purpose or base stations.. However, it's necessary that the network should be secure [1]. Security in Wireless sensor Network is extremely arduous because of its lack of centralized organization and dynamic infrastructure and most vital is Energy. It's extremely potential that some malicious or misbehaving node came into the network or some nodes within the network become malicious, compromise the system practicality and create the system insecure. During this state of affairs it's essential to find the misbehaving node and take away it from the network. tasks. The primary contribution of this research is to classify the recent problems that rely upon capability of attackers, attacks of records in transmission and based on network layers [3].

Manuscript received: 22 May 2020
Manuscript received in revised form: 14 June 2020
Manuscript accepted: 07 July 2020
Manuscript Available online: 15 July 2020

Before going further to define forms of attacks, let's explain the primary and common kind of attack that's recognized as flooding attack.

II. LEACH PROTOCOL

The proposed work done in this paper is basically new concept and this concept is develop in mind of researcher by deep reading of previous research work in security of WSN. In this section we discuss the some previous research work in field of security in WSN.

LEACH protocol is that the 1st protocol of hierarchical routing that proposed information fusion; it's of milestone significance in clustering routing protocol. Routing methods and security problems are great analysis challenge. these days in WSN, numbers of routing protocols are proposed for WSN however most well-known protocols are hierarchical protocols like LEACH. Hierarchical protocols are defined to decrease energy consumption by aggregating information and to reduce the transmissions to the base station. Leach protocol could be a TDMA primarily based MAC protocol. It self-adaptive and self-organized [9].

III. PROPOSED SECURITY SCHEME AGAINST FLOODING ATTACK

The security scheme is completely based on the trust value and better trust value is based not data receiving but due to flooding data packets receiving is minimizes and only few packets are sends and receive in network. The steps of attacker detection and prevention are more evidently mentioned in proposed algorithm. The attacker detection and symptoms are capture by security scheme to block their presence in network. The attacker flooding is totally disappearing in presence of security.

A.Proposed Algorithm

The algorithms steps to identify the flooding attack in network. Parameters for routing are as follows:-

The total number of sensors are = M_i // $i \geq 0$ for all
The number of senders = S_i //
The number of receivers = R_i
Flooding Attacker = M_n
Energy of nodes are considered = E_i
Number of cluster or groups = G_j // $CH_j = G_j$ // // $J \geq 0$ for all
The Cluster Members of $CH_j = CM_b$ //
Range of communication = R_c

Output: PDR, Overhead, Energy consumption, Network Lifetime

Number of nodes is moves with random speed and Election procedure is call by LEACH

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 12, June 2020

{

The M_i nodes are divided in groups $G_0, G_1 \ldots\ldots G_n$

If (M_i Energy = =High && $M_i \leq 550$) // Select Cluster Head having energy is higher than M_{i+1}, M_{i+2}..... M_{i+n} for n next node.

{ CH_j is selected after election

Rest of the nodes of G_J is CM_b }

If ((S_i Next_ Node = = CM_b) && (CM_b !=R_i))

{ Forming CH_j

S_i Sends RREQ and receive RREP till destination is not found

Sends data to receiver } Else

{ Check receiver is exist in other cluster then establish connection sends data or destination is not found }

If ((E_i consumption = high) && (overhead = high) // overhead is more shows more routing packets flooding

{ Check incoming of packets

Check packets contain no data

Attacker M_n presence is confirm } Else

{ Communication is normal and no attacker is exist in network }

In Prevention module proposed security scheme is identified the behavior of attacker and block the attacker malicious activities in network.

If ((M_n packets == unwanated_message) && (message flooding $\geq$ 4*Data rate)

{ Packet receiving is negligible

Junk of packets having no destination

No information of S_i and R_i

Attacker M_n is detected }Else

{ No attacker is exist and sending data to CH_j or CM_b for success delivery }

If ((Packet type = = No information) && (packets incoming = = False))

{ Block the attacker presence;

Disable the communication capability of M_n Broadcast the M_n attacker node_id information in network } }

The proposed approach is also alert the other nodes about the malicious actions of attacker in network. suppose in future attacker is again active in network in that case also the normal nodes are not accepting the data from it. The proposed algorithm approach is to prevent network from attacker because after detection it is necessary to secure routing performance.

IV. SIMULATION PARAMETERS

The analysis is allotted mistreatment network simulator-2 version 2.34 (NS2- 2.34). It's one among the foremost wide used industrial simulators supported Linux platform also produce Linux setting in windows to install Cygwin setup. The final parameters of Network parameters are listed in Table 1.Simulation parameters are considered as number of nodes 30, 40, 50, 60, Propagation is Two ray ground, Antenna is Omi-directional, Transmission range is 550 meters, Traffic type is TCP and UDP, Packet size is 1024bytes, Nodes initial energy is random, Transmission Energy is 1.5 J, Receiving Energy 1.0 J, Idle Energy and Sleep energy0.0J are .0175 J.

V. RESULT ANALYSIS

The proposed protocol is provides the better results due to lesser flooding of unwanted packet and maintain the strong connectivity of nodes in the established path.

A.Performance Comparison of Overhead

In this graph 1 the routing packets flooding in proposed prevention scheme is minimum that' why energy consumption is also reduced. The routing packets are also consuming energy and if the flooding is minimum then in that case the energy is also saved. In TESDA and proposed Prevention the routing overhead is not much more.

Fig 1. Overhead Analysis

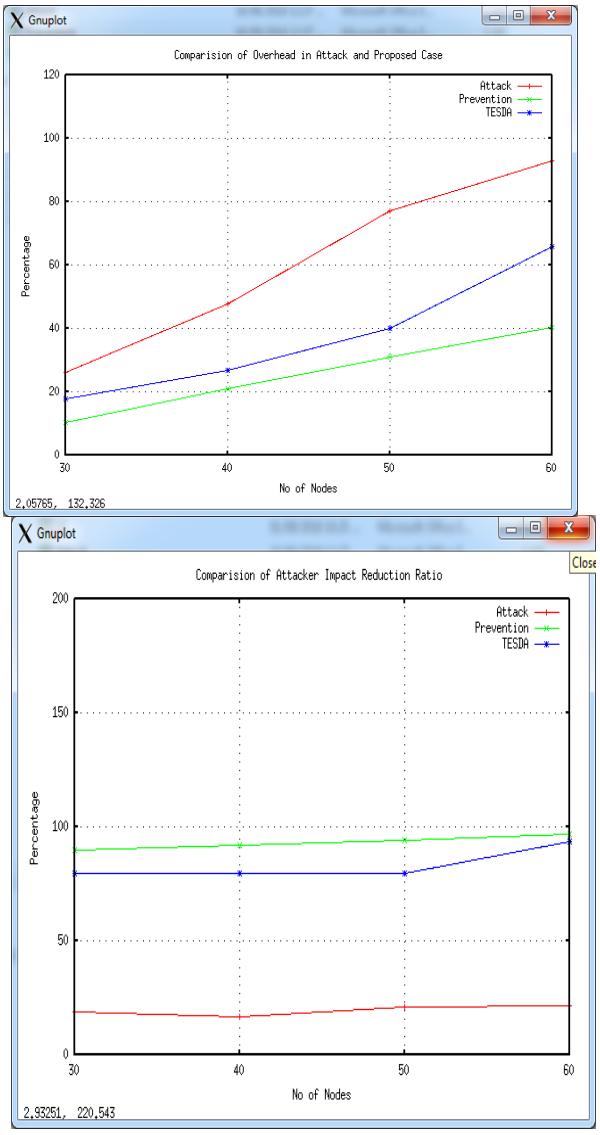

Fig.2 Attacker Impact Ratio Comparison

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 12, June 2020

B.Performance Comparison of Attacker Impact Ratio

The degradation in performance means that 70%. The performance of TESDA is improves the performance and reaches to more than 90% successful transmission and reducing drop percentage. The proposed Prevention scheme is improves the more performance in each node density scenario in network. The proposed scheme is reduces the packet dropping and provides output more than 95% in WSN.

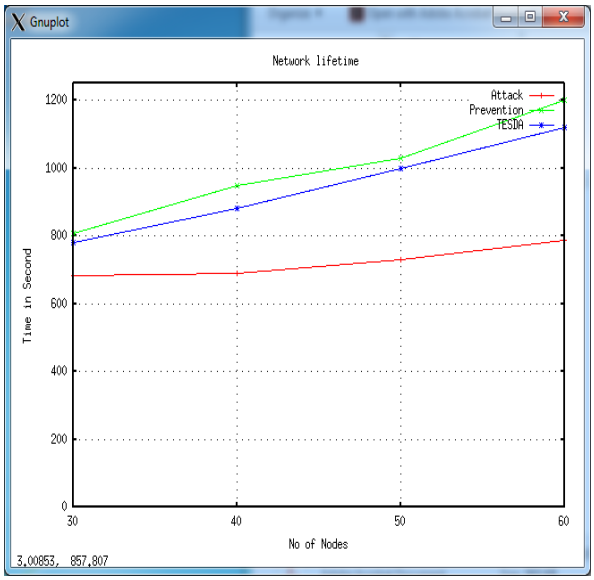

Fig. 3 Network Lifetime Analysis

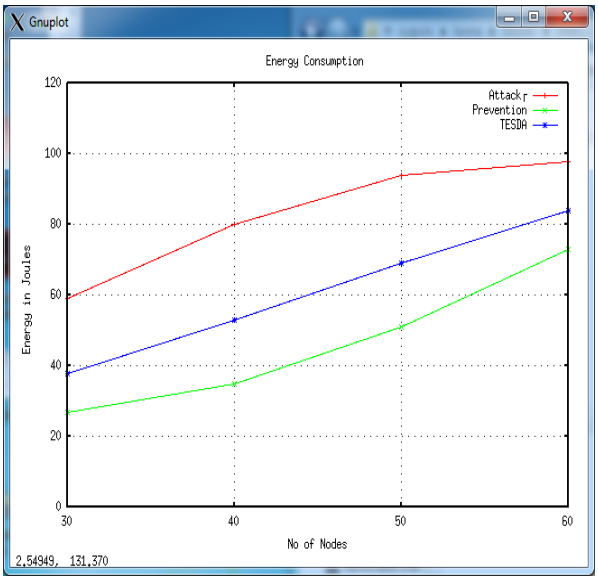

Fig.4 Energy Consumption Analysis

A.Performance Comparison of Network Lifetime

In this graph 3 the live nodes quantity in proposed modified prevention scheme is more that show the nodes are ready to work more time in network in which rest of two protocols performance is showing degradation in each node density scenario.

B.Performance Comparison of Energy Consumption

In this graph 4 the energy consumption of nodes are evaluated in different nodes scenarios. The energy of nodes in network is more in proposed Prevention scheme and the rest of protocol like TESDA and flooding attacker energy consumption is more. The attacker presence in network is consumes the lot of energy because of that the cluster formation and routing procedure are affected and unwanted packets quantity is consumes unnecessary energy

VI. CONCLUSION AND FUTURE WORK

The performance of proposed Security Scheme against flooding attack is more as compare to TESDA existing protocol. The packet receiving is network is also improving the PDR and reduces the packets drooping. If the link establishment is strong then the routing packets flooding is also minimizes that is minimum in proposed modified LEACH approach. The flooding attacker presence in network is showing degradation in routing performance. The energy consumption in proposed scheme is less that shows the better network lifetime. The improved lifetime is shows extra benefit and this benefit is utilized for further communication.

In future we will propose the energy efficient approach to select the node having sufficient energy and reduce the flooding packets energy consumption by form a new mathematical equation. In this equation the energy consumption of node selected having more degree for routing is consider for communication. Also apply this scheme in dense and light network.

REFERENCES

[1] R. Vijayarajeswari, A. Rajivkannan, J. Santhosh ,"Survey Of Malicious Node Detection In Wireless Sensor Networks" International Journal of Emerging Technology and Innovative Engineering , June 2016.

[2] Tarun Bala *, Varsha Bhatia, Sunita Kumawat, Vivek Jaglan "A Survey: Issues and Challenges In Wireless Sensor Network", International Journal of Engineering & Technology, 2018.

[3] M. Roopak, T. Bhardwaj, S. Soni, G. Batra, "Review of Threats in Wireless Sensor Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, 2014.

[4] Priyanka Rawat, Kamal Deep Singh · Hakima Chaouchi, Jean Marie Bonnin, "Wireless Sensor Networks: A Survey On Recent Developments and Potential Synergies", The Journal of Supercomputing, Volume 68, Issue 1, pp 1–48, April 2014.

[5] V. Potdar, A. Sharif, and E. Chang, "Wireless Sensor Networks: A Survey," 2009 International Conference on Advanced Information Network Application Work. 2009 pp. 636–641.

[6] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," Computer Communication., Vol. 30, No. 7, 2007, pp. 1655–1695.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 12, June 2020

[7] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," IEEE Third International Conference on Computer Intelligent Model Simulation, 2001, pp. 308–311.

[8] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless Sensor Networks and the Internet of Things: Selected Challenges," Structural Heal Monitoring. Vol. 5970, 2009, pp. 31–33.

[9] Bhakti Parmar, Jayesh Munjani, Jemish Meisuria, Ajay Singh ",A Survey of Routing Protocol LEACH For WSN " International Journal of Scientific and Research ,2014

[10] P.Padmaja, Dr.G.V.Marutheswar, "Detection of Malicious Node In Wireless Sensor Networks", 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), Jan. 05 – 07, 2017, Coimbatore, INDIA.

[11] 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).