Efficient Robust Routing Protocol (ERRP Model) to Protect WSN under DoS Attacks

Bablu kumar Mishra[1] Prof. Sunil Malviya[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Sagar Institute of Research & Technology, Bhopal, India

Abstract— We knew that there various types of WSN protocols has been proposed from many research proposals time to time to enhance the services and security from different attacks like Hello Message Attack, Flood Attack and DoS attacks , in this paper we concentrate on among multiple is DoS attack, since DoS attack is a very famous category which gets affect system performance simultaneously using fake node such node need to be identify before getting control over the origin server and to avoid DoS situation we design a new protocol called Efficient Robust Routing Protocol which manage sensor network along with shield based networking framework to get eliminate unauthorized access of original server node through intermediate intruders ,so that our primary objective is to detect such intruders nodes before connection and to improve routing efficiency in WSN network. In this paper we carried out the result of proposed algorithm using NS2 simulator to get evaluate performance parameters.

Key words: DoS Attack, WSN, Hello Message Attack, Flood Attack, Efficient Routing

I. INTRODUCTION

Proposed model has been designed for the sensor based communication system which generate the Hello message broadcasting to manage node to node packets transmission and verification of specific sensor node availability in communication range using such hello message techniques sensor node find the destination and its neighbor location details at the end WSN designed the list of intermediate nodes so that information can be deliver up to its destination using intermediate nodes sometimes such designed route has been get influenced by some DoS attackers where WSN network has been completely caught by some unauthorized outsider who get control over it complete over it , in this way someone else will attack to the original server and frequently gets connect the various unauthorized server and client that will gets down the performance factor of data delivery server at the same time as the time gets increased server going to affect with various quality of service factors that has been major defaulter and possibly it is creates more high risk over the server having confidential data , ERR resolve the issues using shield node techniques to immune the network from DoS attack as well as from Hello Flood Attack

Our proposed method will follow following phases during process in WSN:

A. Key Management Setup

This phase plays an important role during WSN communication since during process the distribution of key is very important , key distribution take place using a process called bidirectional and key exchange procedure to get safely distribute the key to broadcast the data or information to the correct sensor node that will managed through session and using such key policy one can gets translate the massage to avoid Flooding over the process of communication and the remaining part of such process has to been gets complete through the exchange of key to avoid unauthorized accessing to the original server and the secure communication with node range.

In bidirectional key setup process every sensor node will generate a broadcast message in its communication range after that node will wait to get another assign message from expected node so that all the nodes having such bidirectional communication link always reply assign message against to every requested message. Due to flood sometimes such message has been dropped out.

As shown in fig. 1 we can say that here sensor node has n number of neighbor it may possible that among such node any node can be an attacker nodes as we can seen in fig. 1 ,here when every node received ACK message , every node will provide an assign message back to the source node aw part from the other unknown node it may be attacker node here we propose an new thing in which to avoid the attacker node to be get contacted through the network we will detached the communication links to protect our network from DoS attack.

B. Routing Process Setup

In this phase the entire active node will be initialized with their neighbor nodes to get connect and create a shielded area for the communication process and going through the shield node specific paths in order to avoid the redundant node interaction during process and to process the RTS and CTS packets to be captured through the internal process of overall WSN communication system. This is the major part of proposed scheme since during routing in sensor nodes, there is a maximum possibility of having an attack of Hello Message and Flood with DoS types of attack that affect the overall performance of specific WSN network.

C. Key Exchange Setup

As long as the verification of communication channels has been done among all the nodes another special mechanism has been needed to create more secure communication environment so that methodology has been involved for this where encoding and decoding has been done using exchange of sensor node keys with their own zoon.

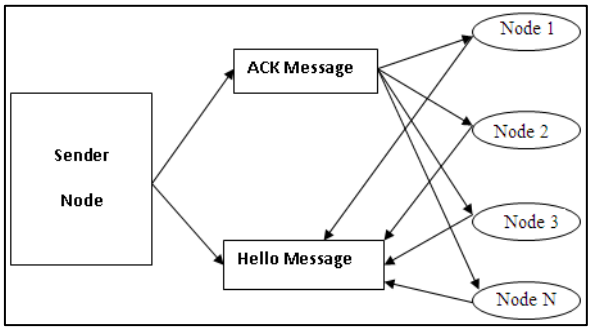

Fig. 1: Process Diagram of Key Exchange Setup

Our approach is to set up shield servers essentially proxies that forward connection requests to the actual server. The connection filtering is to be done at the shields themselves, not at the server. This makes the whole defense more scalable. If a shield gets taken down, the server is still alive, since attackers cannot access the actual server directly. This method is better since the server gets an extra layer of defense it is protected by shields, instead of being directly exposed to the world.

II. LITERATURE REVIEW

Latest technological changes in integrated WSN nodes and circuit mechanism created it attainable for the preparation of little, cheap, low-power, distributed devices to be capable of native process and wireless communication [1]. Such little devices area unit known as sensing element nodes, that area unit capable of solely a restricted quantity of process. however once as the nodes are coordinated with the energy level of multiple WSN interface connections from a variety of different nodes, they have the ability to live a given physical surroundings in nice detail. Thus, a wireless sensing element network may be delineated as a assortment of sensing element nodes that coordinate to perform some specific action. in contrast to ancient networks, wireless sensing element networks rely on dense preparation and coordination to hold out their tasks. During this Chapter, special care is crazy the challenges for this wireless sensing element network. This Chapter mentioned the WSNs analysis, characteristics, design, protocols, applications, security and recommended mechanisms, that lead North American country to what the gaps between this and future challenges that lead this research direction [2].

During the conflict at intervals the 1950's, the United States Navy had trouble locating soviet submarines owing to the shortage of underwater visibility. in that regard they developed a mesh of connected hydrophones referred to as the Sound television system (SOSUS) to seek out these submarines. SOSUS was a system that used Associate in Nursing underwater acoustic sound transducer, hydrophone to seek out the nearest submarines, that is believed of one of the first huge scale Wireless device Networks [5].

The Defense Agency referred to as (ARPA) has begun the use Arpanet between nodes at intervals the Eighties. the thought was to use sort of communication to allow many low worth sensing nodes to be distributed over a larger area with each node operational autonomously victimization this type of communication as a element deciding where the info collected was best used [6]. In the early Nineties beneath the Cooperative Engagement Capability, the U. S. Navy place in a very greenhorn system that used the perceived information from various close to vessels, to produce a clearer image of the target. This communication between the vessels extended vary that the military service vessels might observe and engage from. This communication between the vessels extended vary that the military service vessels might observe and engage from [9, 10].

Wireless detector Networks have been applied to vary of applications, observance of space that includes environmental and surround observance, indoor climate management, and police investigation. Observance things example are typically written as structural observance, condition-based instrumentality maintenance [8]. To boot, observance the interactions of things with each other and additionally the shut space e.g., emergency response, disaster management, healthcare, energy sector [3, 4]. The majority of these applications are additionally split into a pair of classifications: info assortment and event detection.

III. PROPOSED ALGORITHM

In sensor based network, communication may take pace an important part when all the shield based sensor node get interact to each other where ever active shield station needs send identified data or information to other intermediate base station, during this process many time there is a chance of finding some other specific nodes that may be an intruder or else it can be the part of straightforward active zoon of origin server or other participated nodes in this case we use algorithm 1 to take the responsibility of finding such sensor node for the elimination of attack free WSN network.

A. Algorithm 1

- Initialized all the Nodes, Shield Nodes, Target node (Original Server), along with its initial values.
- Now enabled Shield server nodes to get accept and reject connections with original server node.
- Maintain cache node to manage wait for connection states. For all the upcoming and current connection requests.
- To verify connection authentication perform auto authentication process via shield nodes to check:
- Whether Source exceeds its connection limit? If yes then it reject the connection request since it may be DoS client, otherwise go to next.
- Check whether Source exceeds its bandwidth limit? If yes then again the shield node will reject the connection request since it may be DoS client otherwise the request has been accepted for further connection process and data accessing permissions.
- Client would be acknowledged and accepted for the connection with original target server.
- Connection established.
- Receive server response.

IV. FLOW OF DATA FORWARDING PHASE

As we discussed in our methodology that our primary objective is to focused on the identification, detection and verification of all the nodes which we can classify in trusted

and distrusted nodes , we observe in our method that when the requirement of nodes as per the traffic pattern is greater the maximum allowed capacity, in this case if minimum value allowed for traffic pattern is sensor node can be intruders or suspicious , which comes into the category of distrusted node otherwise remaining all the node will li1sted as trusted as mention in fig. 2.

As mention in above fig. 2 data flow process has been going to get detect the selfish and non-selfish nodes by comparing traffic flow with allowed traffic value so that we can identify and attacker's nodes.

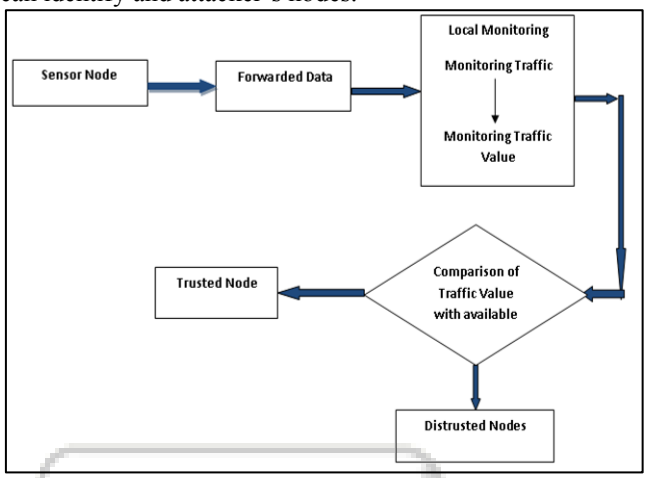

Fig. 2: Process Flow for Data Forwarding & Detection of Trusted & Distrusted Node

V. EVALUATION OF PROPOSED MODEL

In this section we simulate and perform series of experiments with varying numbers of sensor nodes with different traffic intervals , all the nodes has been associate with the simulation area of 1000×1000m. Random walk has been generated with CBR over source and destination, to get simulates the series of experiments for comparison of result following simulation parameters has been used which is listed below in Table 1.

Parameter Type	Parameter Value
Simulation Time	60ms
Simulation Area	1000×1000m
No of nodes	10,20,30,....50
Walk	Random Walk
Antenna Type	Omni Antenna
MCA Protocol	802.11
Transmission Range	250m
Traffic Model	CBR

Table 1: Simulation Parameters

The process parameters gathered by performing and computing the different ratio like packet delivery ratio (PDR), End to End delivery ratio for computing delay factors as well as the computation of routing throughput.

To determine systems nature we compute PDR so that system fluctuation can be major at run time processing environment, it also defines the overall framework of the system. Following majors and parameters has been carried out using Packet Delivery Ratio.

PDR=Number of Packet Delivered/Time

In following fig. 4 we can discuss the Packet Delivery Ratio under DOS attack condition , in which practical implementation of proposed code demonstrate the result of ERR algorithm in superior way, here we can see that higher packets delivery ratio define the elite status of current system, fig.3 describes different resulting parameters for the presentation of different ratio another important concept which we got after simulation about packet loss ratio is it is use to define the overall nature of the system with shield node , fig. 4 also bring the effect of packet loss ratio which shows higher performance of the system .

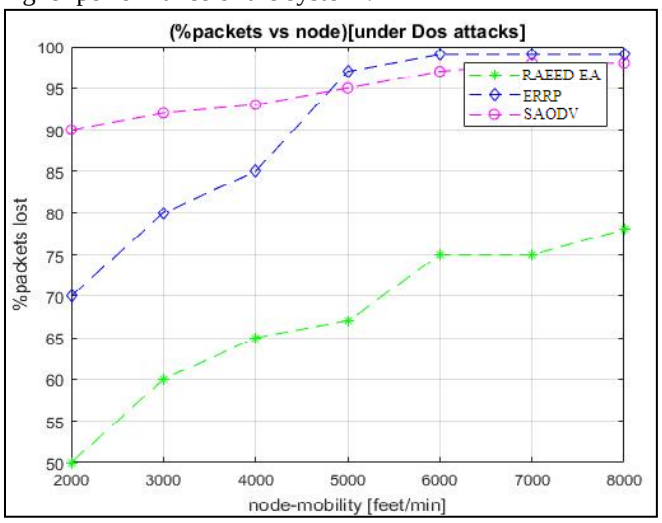

Fig. 3: Demonstration of Packet Delivery Ratio under DoS Attack

On the other hand in fig. 4 demonstrate that total time took by the sender node to transmit the data efficiently to the desired destination it has been compute and majored in network term called End to End Delay consideration using following equation we perform End to End delay.

End To End Delay=Packet Arrival Time-Packets sent Time/Number of Connection

fig. 4 demonstrate the resulting parameters of proposed model for End to End delay , here we graphical analysis defines that proposed scheme maintain manage with tolerated End to End Delay in WSN.

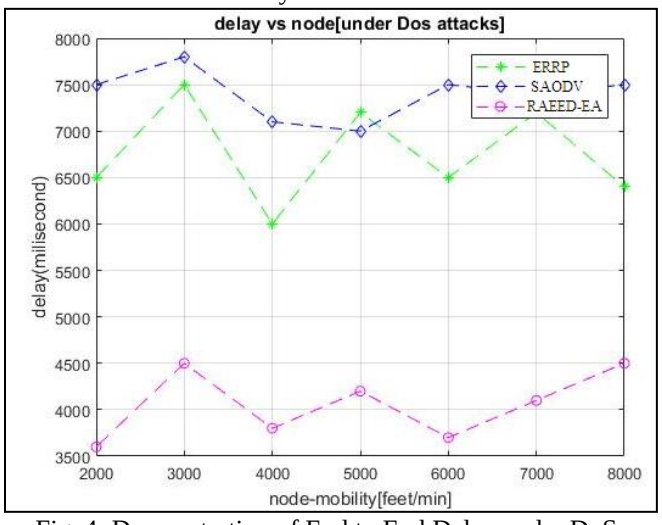

Fig. 4: Demonstration of End to End Delay under DoS Attack

Whereas throughput is another important variant to be discussed in fig. 5 which describes that total amount of Data Packets need to be sent to the desired destination in specific per unit of time. In our approach throughput measurement and computation has been done using following formula:

Throughput =Number of Packets Delivered/ Time Period

In fig. 5 shows proposed algorithm defines that system provides higher throughput in result we means with variant number of nodes and different traffic pattern value system throughput has managed and provides efficient and secure correspondence for sensor based network under DoS attack circumstances.

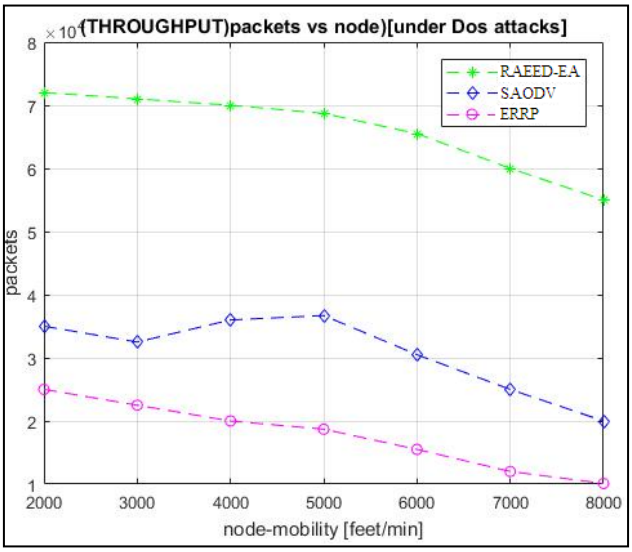

Fig. 5: Demonstration of throughput under DoS Attack

VI. CONCLUSION

As discussed in previous section that proposed secure ERR scheme perform well under DoS attack condition with different traffic pattern and values, our proposed scheme answers for different attack in study with NS2 simulation. The used scheme utilize the bidirectional Omni antenna phase with check point technique from distance for transmission of data packets against Hello Message attack and Flood Attacks, it defines safe and secure communication, verification and also maintain authorization of nodes under attack possibility, using this scheme we got very good results for the point of view of performance, efficient and security in under DoS attack condition.

REFERENCES

[1] T.R. Andel et al., Automated evaluation of secure route discovery in MANET protocols, pp 26–41. Springer, 2012.
[2] Y. Hanna, et al., A domain-specific verification framework for sensor network security protocol implementations. In Proceedings of the first ACM conference on Wireless network security (WISEC '08), Alexandria, VA, USA, pp 109–118, 2013.
[3] K. Saghar. Formal Modelling and Analysis of Denial of Services Attacks in Wireless Sensor Networks. Ph.D. dissertation, School of Computing and Engineering, Northumbria University, Newcastle upon Tyne, UK, 2014.
[4] Henderson,et al., Formal modelling and analysis of routing protocol security in wireless sensor networks. In PGNET '09, pp 73–78, 2010.
[5] K. Saghar, W. Henderson, D. Kendall, and A. Bouridane. Applying formal modelling to detect DoS attacks in wireless medium. In IEEE, IET International Symposium on Communication Systems, Networks And Digital Signal Processing Nasa/Esa (Csndsp 2018), 2018.
[6] W. Henderson, et al.,and A. Bouridane. Formal modelling of a robust wireless sensor network routing protocol. In NASA/ESA Conference on Adaptive Hardware and Systems (AHS- 2010), 2017.
[7] D. Kendall, et al., Vulnerability of INSENS to denial of service attacks. In 36th International Conference on Acoustics, Speech and Signal Processing (ICASSP 2011), Praha, Czech Republic
[8] K. Saghar, et al., Automatic detection of black hole attack in wireless network routing protocols. In IEEE, International Bhurban Conference on Applied Sciences & Technology Islamabad, (IBCAST 2014) Pakistan, 2014.
[9] L. Tobarra, et al., Formal analysis of sensor network encryption protocol (snep). In IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), Piscataway, NJ, USA, pp 767–772, Pisa (Italy), 2016.
[10] D. Cazorla, et al., Model checking wireless sensor network security protocols: Tinysec + leap. In Proceedings of the First IFIP International Conference on Wireless Sensor and Actor Networks (WSAN'07), pages 95–106. IFIP Main Series, Springer, 2015.

