A Novel Robust Routing Protocol RAEED to Avoid DoS Attacks in WSN

S.Uma maheswari
ME (CSE) student
S.A Engineering College
Chennai
uthra276@gmail.com

N.S.Usha
Associate Professor
S.A Engineering College
Chennai
sushak3001@yahoo.co.in

E.A.Mary Anita
Professor
S.A Engineering College
Chennai
drmaryanita@saec.ac.in

K.Ramaya Devi
Assistant Professor
S.A Engineering College
Chennai
ramyadevik@saec.ac.in

Abstract—**Many of the WSN routing protocols are vulnerable to DoS attack such as Hello Flood Attack, Sink hole and Black hole attack etc. In this paper, we are principally focus on one attack among these is Hello Flood Attack. Some directing conventions need to show Hello Message intermittently to its neighbor nodes. The nodes get this welcome message accept that the sender is in its extent. This welcome message might prompts Hello Flood attack to prevent this attack in WSN, we propose a new secure routing scheme called as Robust formally analyzed routing protocol for wireless sensor network deployment (RAEED). In this scheme, improved Bidirectional verification scheme is used to rectify the Hello Flood Attack in WSN. The computer simulations were carried out by using Network Simulator (NS2) to evaluate the performance of our routing scheme.**

Keywords—Wireless Sensor Networks (WSN), Denial of Service attack (DoS), Hello Flood Attack, and Bidirectional Verification Scheme .

I. INTRODUCTION

Wireless Sensor networks are most widely used for the critical applications such as Military applications, Environmental applications, and Health applications etc. In Military field, the WSN is used for battle damage valuation, Scouting of opposing forces and to detect the biological and chemical attack. Environmental applications comprises trajectory the movement of insects and small animals and irrigation monitoring etc. In the medical field, it is used to monitor the patients and to track the doctor location in hospital. So, the security and reliability of data is much more important in WSN.

The WSN is resource limited due to limited processing speed, power, memory and bandwidth. Inventive techniques are required to overcome these limitations. Each wireless node is having its own communication range. The wireless sensor node can directly send the data from one node to another which are present in the range. If the supposed destination is out of range within the feel, the source node has to relay the data packets through other nodes. This process is called as routing. The routing protocol designed for WSN should consider the resource limited nature of sensor nodes.

Because of the limited resources of sensor, broadcast characteristics of transmission and unfriendly environment of WSN numerous attacks are possible. The attacker node in the WSN can easily overhear the broadcast transmission between the sensor nodes. Sometimes, the attacker may modify the data or leads to false data injection. WSN routing is vulnerable to DoS attack which includes Hello Flood Attack, Black hole/Gray hole attack, Jamming attack, and Spoofing attack etc.

To moderate the susceptibilities of WSN routing scheme, we propose a secure and efficient routing scheme named as Robust formally analyzed routing protocol for wireless sensor network deployment (RAEED). In this paper, we are mainly concentrating on the Hello Flood attack in WSN. RAEED not only provide the solution to Hello Flood attack but also provide the solution to other DoS attack. The rest of the paper is organized as follows: section I discuss the various existing works related to our proposed work. Section II elaborately explains the steps involved in the proposed scheme. The simulation results are displayed in section III. Section IV concludes our proposed scheme.

II. RELATED WORK

The WSN is helpless against DoS attack due its telecast nature of transmission and hostile environment. The Hello Flood attacker will make harm to the WSN while recognizing the neighbor nodes. The Hello Flood attack causes the unidirectional link between the attacker and the legitimate or normal nodes in the network. The researchers have proposed solution for such attack is called as Hello Flood attack and Defense scheme [11]. The probabilistic secret sharing protocol is used to tolerate the damage caused by an adversary. In this scheme, the secret data shared between two sensor nodes are not visible to other nodes. The authors have shown that the defense mechanism against Hello Flood attack can endure the impairment caused by a malicious node.

978-1-5090-2552-7

In [12], the effective security component for substantial scale Sensor systems is proposed. The creators have named the proposed convention as localized encryption and authentication protocol (LEAP). It gives four sorts of keys to every sensor nodes to give the security to various sorts of messages traded between the sensor nodes. They are singular key, pairwise key, bunch key and gathering key. This convention utilizes the restricted hash fasten calculation to give verification and privacy to the messages. It can strengthen source validation without idle commitment. This convention is effective under different attack models. Yet, the quantity of messages traded to give the security is high.

The intrusion tolerant routing protocol for Wireless Sensor Networks is described in [13]. The forwarding table is kept up for every node to empower the correspondence with the base station. INSENS did not focus on recognizing the malevolent nodes in the system, yet decently it endures the vicinity of acting mischievously nodes. The real point of preference of INSENS is the vindictive hubs in the system can trade off a little number of sensor hubs just, the aggressor can't establish to broad harm in the system. To keep away from these issues, we propose a safe and productive routing scheme Robust formally analyzed routing protocol for wireless sensor network deployment (RAEED) to give the safeguard against DoS attack in WSN directing.

III. PROPOSED METHOD

The vast majority of the steering conventions in the remote sensor system telecast the Hello message in the system to know the hubs those are available inside its correspondence range. The nodes which are receiving this Hello message assume that, the sender of this hello message is available within its range. This is a modest way used by WSN to discover the list of neighbors to forward the information towards the planned destination. A few times this humble path prompts Hello Flood Attack in Wireless Sensor Networks. For this, we proposed a steering plan called Robust formally analyzed routing protocol for wireless sensor network deployment (RAEED). This coordinating arrangement not simply gives the course of action against Hello Flood Attack furthermore give the game plan against various DoS attack in Wireless Sensor Networks. In this portion, we are going to discuss this proposed arrangement.

Our proposed routing scheme is alienated into following 3 phases:

- Key setup phase
- Route discovery Phase
- Data Transmission Phase

Key setup phase

This phase plays an important role to remedy the Hello Flood Attack in Wireless Sensor Networks. This phase is further subdivided into Bidirectional verification phase and Key interchange phase.

Bidirectional verification Phase

In this phase, each sensor node broadcasts the ASK message within its range and wait for receiving ASSIGN message from that nodes. The nodes which are having bidirectional link send the ASSIGN message back to the sender of ASK message. This process is explained by figure.1. If any malicious node (Hello Flood Attacker) receive this ASK message, it never send the ASSIGN back to the sender node due to its flood nature.

In the figure.1, Assume that, a sensor node has ‘n’ number of neighbors. Among these neighbor nodes, one node is an attacker node. After receiving ASK message, each node send the ASSIGN message back to the sender of Hello message except one n-1th node (Attacker node). To exclude the attacker from the network, all the unidirectional links are detached. Thus the Hello Flood Attack is removed in this phase.

Key interchange phase

After verifying the bidirectional link between the nodes, the keys used for the encryption and the decryption of messages is exchanged between the nodes in the range. The keys are traded with the hubs those are send the ASSIGN message back to the sender hub.

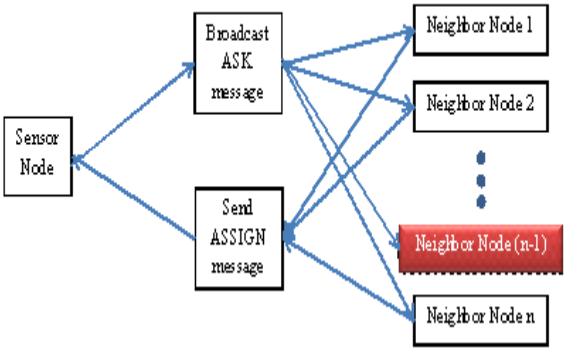

Fig 1 Block diagram of key setup phase

Route Discovery Phase

In the WSN, every sensor hub needs to send its detected data to the Base station/Sink, on the off chance that it identifies an occasion. In the event that the Base station is accessible inside the correspondence scope of a sensor hub in the sense the sensor can send the information straightforwardly without the backing of whatever other hubs in the system. Else the sensor hub needs to send the information through some middle of the road hubs. The determination of middle of the road hubs to send the information to the planned destination is called as route. If the intermediate node is a malicious node, it will leads to false injection attack in WSN. The accuracy of the data should be maintained as Wireless Sensor Network is mainly used for critical applications. To avoid these problems, our secure routing scheme the data is transferred through verified neighbors detected in Key Setup Phase. The route discovery phase is elucidated by algorithm 1

By using the algorithm1, every sensor node S_{id} finds the valid hop separation from Base station "BS" $A_{hd(BS\to S_{id})}$. The data to this computation is affirmed 1 hop neighbors V_{1hn} and 2 hop neighbors V_{2hn} verified using Key Setup Stage. N_n Shows the accompanying node in the course to accomplish the Base station. In case the Base station is in the 1 hop neighbors of sensor node S_{id}, then it can particularly transmit the data. Along these lines, the authentic hop distance from the base station is 1.

Algorithm 1

Input: S_{id}, V_{1hn}, V_{2hn}

Output: $A_{hd(BS\to S_{id})}$

$N_n = S_{id}$

$A_{hd(BS\to S_{id})} = 0$

While N_n ==BS do

If BS is in V_{1hn}

N_n =BS

$A_{hd(BS\to S_{id})} = A_{hd(BS\to S_{id})} + 1$

Else if BS is in V_{2hn}

N_n =BS

$A_{hd(BS\to S_{id})} = A_{hd(BS\to S_{id})} + 2$

Else

For each node n1 in V_{1hn}

If node n1 has minimum distance to BS

N_n =n1

$A_{hd(BS\to S_{id})} = A_{hd(BS\to S_{id})} + 1$

End if

End for each

End If

End While

Return $A_{hd(BS\to S_{id})}$

If the Base station is in the 2 hop neighbors of node S_{id}, in the sense the authentic hop distance is 2. Else, we have to pick the accompanying hop node N_n from the list V_{1hn}.The node which is having slightest partition to the Base station is picked as the accompanying hop node. This methodology continues until it recognizes the Base station. For each and every widely appealing node the dependable hop detachment $A_{hd(BS\to S_{id})}$ expanded by 1. Finally this count gives back this worth $A_{hd(BS\to S_{id})}$. The widely appealing nodes are looked over the checked 1 hop neighbors V_{1hn} in perspective of the partition to the Base station. Along these lines, the sink hole attack and false mixture attack in the WSN is change in this stage.

Data Forwarding Phase

Hence, dispense out the reliable hop separation from base station to each sensor nodes in the framework the data distinguished by the sensor node is sent to the base station. While sending the information, the sensor hubs do Local Monitoring and rank its neighbors as per the information sending execution. Neighborhood checking procedure has been demonstrated to enhance the security in multihop Wireless Sensor Networks. When the sensor node monitors the traffic of its neighbors, it can estimate the traffic value of each neighbor node. The Traffic value of neighbor node is denoted by TV_{neigh}. Based on this monitored traffic value, the neighbor nodes are ranked. The maximum allowed traffic of node which is monitoring its neighbors is denoted by $TV_{\max}$ and the minimum allowed traffic of node which is monitoring its neighbors is denoted by $TV_{\min}$

$$TV_{neigh} > TV_{\max} \otimes TV_{neigh} < TV_{\min} \qquad (1)$$

The neighbor nodes are ranked as trust node and distrust node by check the condition in (1). The traffic value of neighbor node is greater than the maximum allowed traffic or lesser than the minimum allowed traffic means that particular sensor node is a suspicious or distrust node. Else that neighbor node is a trustable node as explained in the figure.2.

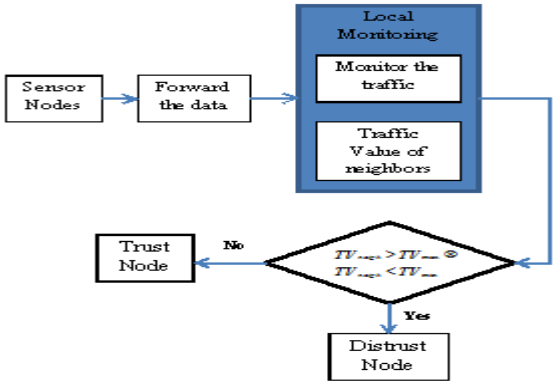

Fig 2 Flow Diagram of Data forwarding Phase

From this Data Forwarding Phase, we can detect the selfishness of the nodes if the traffic flow is lesser than the minimum allowed traffic. Also, we can detect the Black hole and Gray hole attacker in the route by local monitoring results.

IV. EVALUATION OF RAEED

We conduct a series of experiments by varying data transmission interval. The nodes are distributed in the simulation area of 1500×1000m. The UDP/CBR (Constant Bit Rate) traffic is generated between the source and destination. The data packets are scheduled after 0.05ms. The detailed simulation parameters are listed in table1.

TABLE I
SIMULATION PARAMETERS

Parameter Type	Parameter Value
Simulation time	60ms
Simulation area	1500×1000m
Number of nodes	10,20,30…,50
Path loss model	Two Ray Ground
Antenna Type	Omni Antenna
Mobility Model	Random Way Point
MAC protocol	802.11
Transmission range	250m
Traffic model	CBR

The NS2 Simulator is predominantly utilized as a part of the examination field of systems and correspondence. The NS2 is a discrete occasion time driven test system which is utilized to assess the execution of the system. Two dialects, for example, C++, OTCL (Object Oriented Tool Command Language) are utilized as a part of NS2. The C++ is go about as back end and OTCL is utilized as front end. The X-graph is utilized to plot the diagram. The execution assessed by utilizing the system parameter packet delivery ratio, packet loss ratio, end to end delay, routing overhead and throughput.

The Packet delivery ratio is the extent of the data groups passed on to the destination adequately. The Packet delivery ratio is one of the basic parameter to evaluate the system nature of the framework.

The formula used to find the Packet delivery ratio is as follows:

$$PDR = \frac{No.\ of\ packets\ delivered}{Time}$$

Fig.3 gives the diagram for Packet delivery ratio. The graph demonstrates that, the proposed plan RAEED gives superior. Higher the Packet delivery ratio demonstrates that the elite of the system.

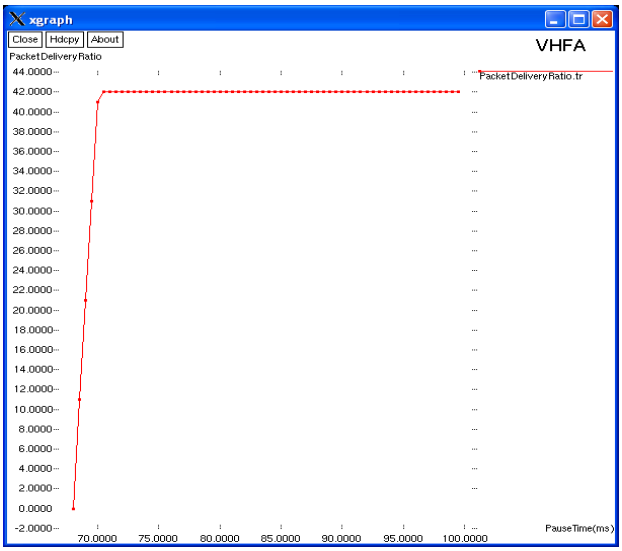

Fig 3 Packet delivery ratio analysis of proposed scheme for various simulation periods

The Packet loss ratio is utilized to assess the nature of the system gave by the steering plan.The packet loss ratio of the proposed plan is zero as appeared in Fig. 4. Bring down the Packet loss ratio that demonstrates that the higher performance of the system.

The time taken by the source hub to convey the information effectively to the destination is called as End to End delay. The accompanying equation is utilized to ascertain the End to End delay.

$$EndtoEndDelay = A_T - S_T / n$$

Where,

A_T →Arrival Time

n →Number of Connections

S_T →Sent Time

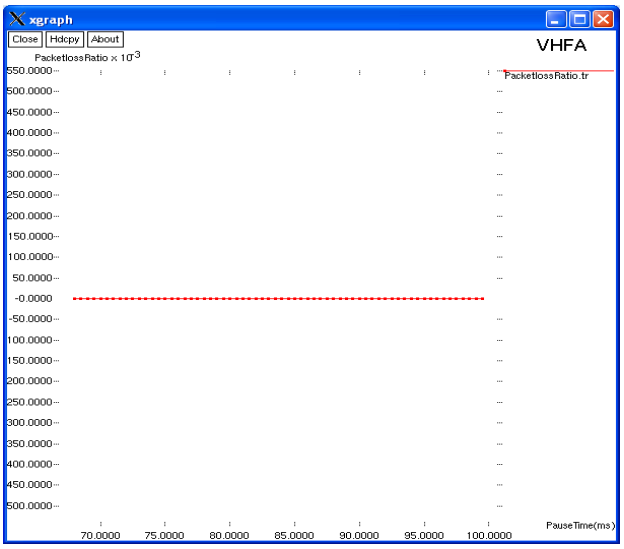

Fig 4 Packet loss ratio of proposed scheme RAEED

Fig. 5 shows that the End to end analysis of the proposed scheme. The proposed scheme leads to only tolerated delay in the network.

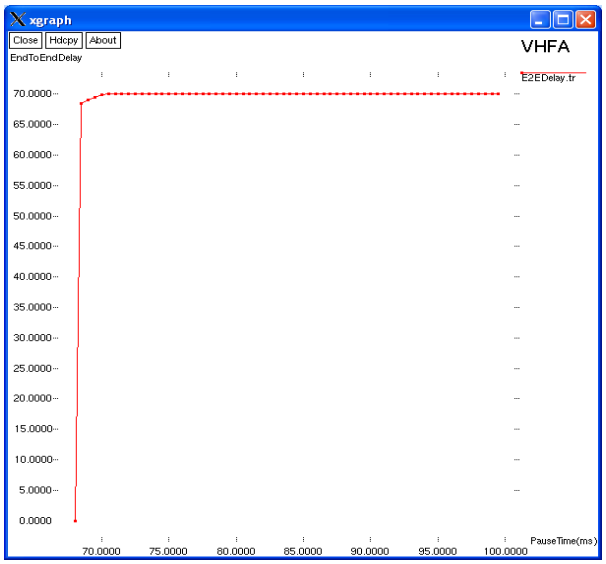

Fig 5 End to End delay analysis of proposed scheme RAEED

Throughput is the amount of packets delivered to the destination per unit of time. The Throughput is calculated by using the formula

$$Throughput = No.\ of\ packets\ delivered \,/\, Time\ period$$

The system provides high throughput as shown in Fig. 6. As a result, the proposed plan ensures effective and secure correspondence in Wireless Sensor Networks.

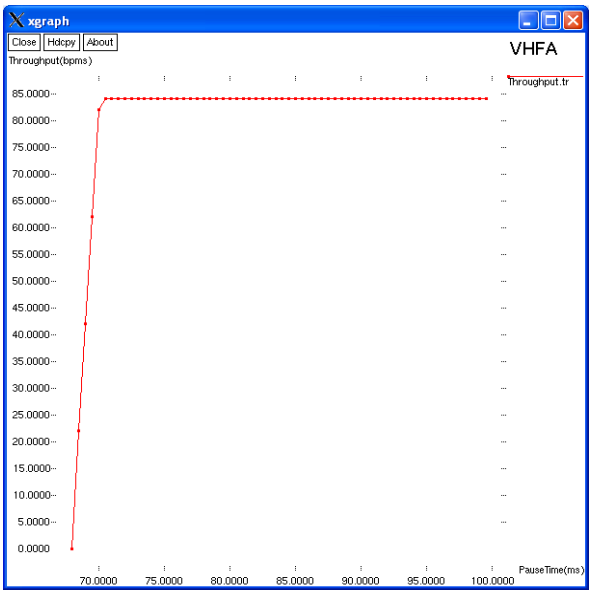

Fig 6 Throughput analysis of proposed scheme RAEED

V. CONCLUSION

The proposed secure directing plan RAEED gives answer for Hello Flood Attack in Wireless Sensor Networks. This RAEED utilizes the enhanced bidirectional check procedure to maintain a strategic distance from Hello Flood Attack. This change offers high security in the meantime decreases movement. The Simulation results demonstrate that, the proposed routing scheme RAEED provide better performance in the presence of DoS attacker. The number of messages interchanged among the nodes and time to complete key setup phase is low for RAEED.

REFERENCES

[1] T.R. Andel et al., Automated evaluation of secure route discovery in MANET protocols, pp 26–41. Springer, 2008.

[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, 2008.

[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, 2010.

[4] Henderson,et al., Formal modelling and analysis of routing protocol security in wireless sensor networks. In PGNET '09, pp 73–78, 2009.

[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 2010), 2010.

[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), 2010.

[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), 2007.

[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, 2007.

[11] M. A. Hamid, et al., Routing security in sensor network: Hello flood attack and defense. In IEEE ICNEWS 2006, Dhaka, 2006.

[12] S. Zhu, et al.,. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In ACM Conference on Computer and Communications Security (CCS'03), pp 62–72, 2003.

[13] J. Deng, et al., INSENS: Intrusion-tolerant routing for wireless sensor networks. In Elsevier Journal on Computer Communications, Special Issue on Dependable Wireless Sensor Networks, volume 29, pp 216–230, 2005.