A Modified Algorithm and Protocol for Jamming Attack Prevention for Wireless Sensor Network

*** Harshita Kothari**
**** Prof. Ashish Tiwari**

ABSTRACT

Wireless networks are gaining popularity to its peak nowadays, because the users need wireless connectivity regardless of their geographic position. there's an increasing threat of attacks on the Wireless sensor Network (WSN). Node jamming attack is one in all the security threat within which the traffic is redirected to such a node that really doesn't exist within the network. It's an analogy to the Jamming within the universe within which things disappear. The node presents itself in such some way to the node that it will attack different nodes and networks knowing that it's the shortest path. WSNs should have a secure approach for transmission and communication that is kind of difficult and very important issue. so as to produce secure communication and transmission, research worker worked specifically on the security problems in WSNs, and lots of secure routing protocols and security measures inside the networks were proposed.

The scope of this work is to review the effects of Jamming attack in WSN exploitation (and prevention this attack exploitation security primarily based modified. Comparative analysis of Jamming attack for each protocols is taken under consideration. The impact of Node Jamming attack on the performance of WSN is evaluated searching for that protocol is additional vulnerable to the attack and the way abundant is that the impact of the attack on each protocols. The measurements were taken within the light of packet delivery ratio, throughput, end-to-end delay and residual energy. Simulation is completed in Network simulator tool two (NS-2).

Keywords: WSN, Jamming attack, AODV Routing Protocols, NS-2.

* Harshita Kothari, Dept. of Software System (VITS), Indore, harshita2508@gmail.com

** Prof. Ashish Tiwari, Dept. of Software System (VITS), Indore

I. INTRODUCTION:

In recent years, advance in micro-electro-mechanical systems (MEMS) that are the integrations of mechanical parts, sensors, actuators and electronics on a typical silicon substrate through small fabrication technology and have enabled low-cost and low-power in electronics and wireless communication technology enabled small sensor nodes to communicate in short distance. Wireless sensor Networks (WSNs) comprise various small sensor nodes that are deployed in spatially distributed terrain. every sensor node is endowed with a restricted amount of process, however once coordinated with the knowledge from different nodes, they need the flexibility to measure the given physical atmosphere in great details or to execute a task with advanced functions. Hence, a sensor network may be represented as a set of sensor nodes that coordinate with one another to perform some specific actions. Since every sensor node is fitted with an on-

board processor, sensor nodes use their process abilities to seek out out simple computations and transmit solely the required information. These features permit the sensor networks to use in several applications, like military, security and atmosphere. Wireless sensor networks can also be deployed within the ways in which the wired sensor system can't be deployed such as within the chemical environments that are inaccessible by humans.

II. CLASSIFICATION OF PROTOCOLS

Routing techniques are needed for sending information between sensor nodes and also the base stations for communication. Completely different routing protocols are proposed for wireless sensor network. These protocols are classified consistent with completely different parameters. Protocols will be classified as supported their mode of functioning and kind of target applications.

- **Proactive.**
- **Reactive.**
- **Hybrid.**

In a proactive protocol the nodes start their sensors and transmitters, sense the atmosphere and transmit the information to a bs through the predefined route. The Low Energy adaptive clustering hierarchy protocol (AODV) utilizes this kind of protocol [7].

In case of a reactive protocol if there are unexpected changes within the sensed attribute on the far side some pre-determined threshold value, the nodes immediately react. this kind of protocol is employed in time important applications. The threshold sensitive Energy efficient sensor Network (TEEN) [8] is an example of a reactive protocol.

Hybrid protocols like adaptive Periodic teen (APTEEN) incorporate each proactive and reactive ideas [9]. They initial compute all routes so improve the routes at the time of routing. Further, consistent with the participation type of the nodes routing protocols may be classified as direct communication, flat and clustering protocols.

AODV (Low Energy adaptive clustering Hierarchy):

AODV [7] may be a self-organizing, adaptive clustering protocol. It uses randomisation for distributing the energy load among the sensors within the network. the subsequent are the assumptions created within the AODV protocol:

- All nodes will transmit with enough power to achieve the base station.
- Each node has enough computational power to support completely different mac protocols.
- Nodes set near one another have correlate information.

According to this protocol, the base station is fixed and located far from the sensor nodes and also the nodes are homogeneous and energy affected . Here, one node known as cluster-head (CH) acts because the local base station. AODV at random rotates the high-energy cluster-head so the activities are equally shared among the sensors and also the sensors consume battery power equally. AODV additionally performs information fusion, i.e. compression of data once data is distributed from the clusters to the base station therefore reducing energy dissipation and enhancing system period of time. AODV divides the overall operation into rounds.

III. PROPOSED PROTOCOL

JAODV (Modified Low Energy adaptive clustering Hierarchy): Low-Energy adaptive clustering Hierarchy (AODV), may be a typical hierarchical clustering routing protocol, that adopts distributed clustering algorithmic rule wherever cluster-head rotation mechanism, information aggregation, and information fusion technologies effectively improves the time period of network. so as to optimize energy within the network, nodes are chosen as cluster head circularly and randomly. the conventional nodes known as cluster members be a part of the corresponding cluster head nodes on the basis of principle of proximity. traditional nodes sense information and send on to the cluster head nodes. The cluster head nodes receive sensed information, aggregate the information to remove redundancy and fusion processes are distributed and data is send to the sink (or Base Station). therefore AODV will increase network time period by decreasing network energy consumption, and reducing variety of communication messages by information aggregation and fusion. the method of formation of clusters in JAODV may be a cluster primarily based hierarchical routing protocol supported MAODV. This protocol is employed for time-critical applications. it's two assumptions:

- The bs and also the sensor nodes have same initial energy
- The bs will transmit information to all or any nodes within the network directly.

In this protocol, nodes sense the medium incessantly, however the information transmission is completed less frequently. The network consists of simple nodes, first-level cluster heads and second-level cluster heads. teenage uses AODV's strategy to create cluster. first level CHs are formed faraway from the bs and second level cluster heads are formed almost the bs. A CH sends 2 varieties of information to its neighbours—one is that the hard threshold (HT) and alternative is soft threshold (ST). within the hard threshold, the nodes transmit information if the detected attribute is within the vary of interest and therefore it reduces the amount of transmissions. On the opposite hand, in soft threshold mode, any small change within the value of the sensed attribute is transmitted. The nodes sense their environment continuously and store the sensed value for

transmission. thenceforth the node transmits the sensed value if one in all the subsequent conditions satisfied:

(i) Sensed value > hard threshold (HT).

(ii) Sensed value ~ hard threshold >= soft threshold (ST).

IV. IMPLEMENTATION AND RESULTS

In this work, the random way point static model is used for the simulation of WSN routing protocols. The source-destination pairs are spread randomly over the network where the point to point link is established between them.

In this work UDP agent with CBR traffic is used with 40 packet size and 10kbps rate used for the transmission. The simulation configuration for static nodes consists of many network components and simulation parameters that are shown in the table in detail.

Network Simulation

Generally network simulators try to model the real world networks. The principle idea is that if a system can be modeled, then futures of the model can be changed and the corresponding results can be analyzed. Following features are provided by simulator.

Table 1: Simulation parameter

Simulation TOOL	**Network Simulator-2.35**
IEEE Scenario	WSN (802.15.4)
Static Model	Two Ray Ground
Number Of Nodes	30,60,80
Node Movement speed	Static network
Traffic Type	UDP
Antenna	Omni Directional Antenna
MAC Layer	IEEE 802.15.4
Routing Protocols	AODV , JAODV , MAODV
Queue Limit	50 packets
Simulation Area(in meter)	2000*2000
Queue type	Drop tail
Channel	Wireless Channel

The following metrics are used in this work for the detection and prevention of the node Jamming attack with AODV routing protocol.

A. Packet Delivery Ratio

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes.

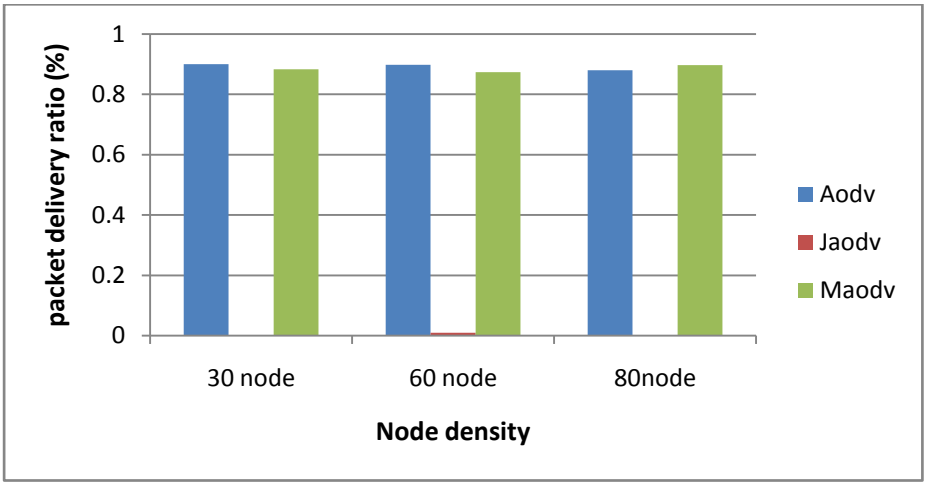

Figure 1: Packet Delivery Ratio under AODV, JAODV and MAODV

Analysis of Packet Delivery Ratio: The fig shows the effect to the packet delivery ratio (PDR) measured for the AODV, JAODV, MAODV protocols when the node Density is increased. It is measured that the packet delivery ratio dramatically decreases for JAODV.

End to End Delay:

This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

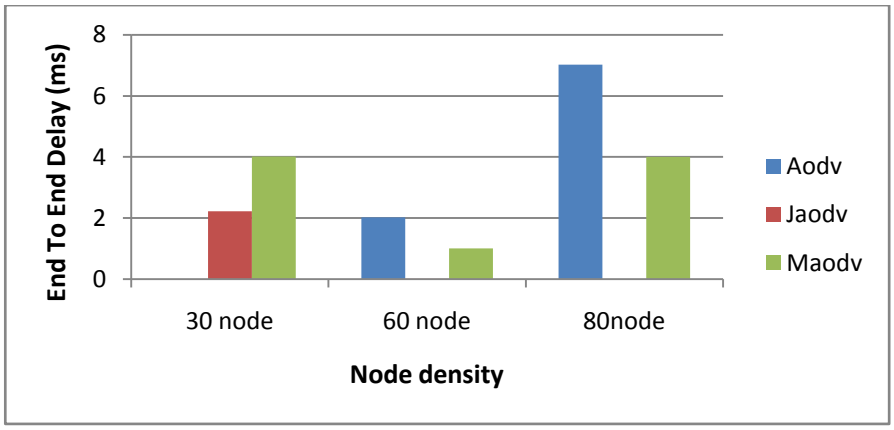

Figure 2: End To End Delay under AODV, JAODV and MAOD

Energy:

This is the average energy between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the energy caused during route acquisition, buffering and processing at intermediate nodes.

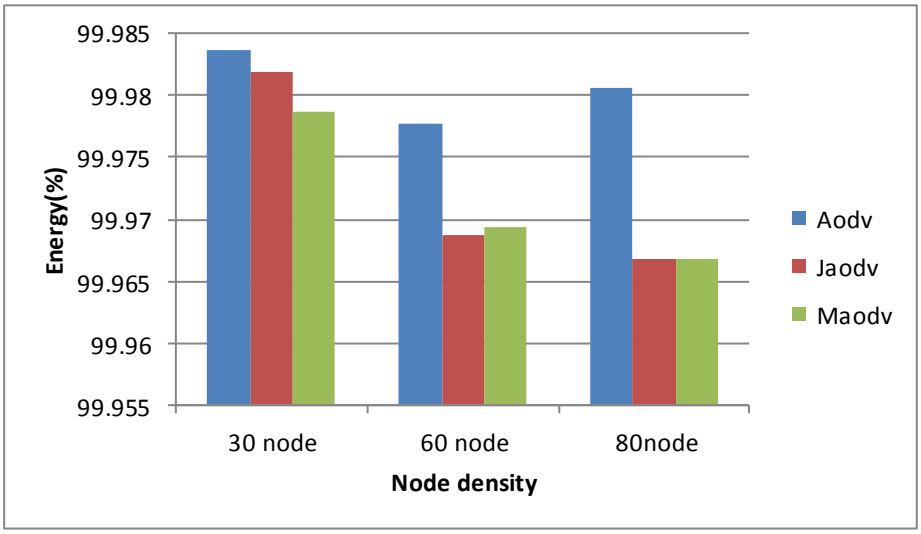

Figure 3: Energy Under AODV,JAODV and MAODV

Throughput:

There are two representations of throughput; one is the amount of data transferred over the period of time expressed in kbps. The other is the packet delivery percentage obtained from a ratio of the number of data packets sent and the number of data packets received.

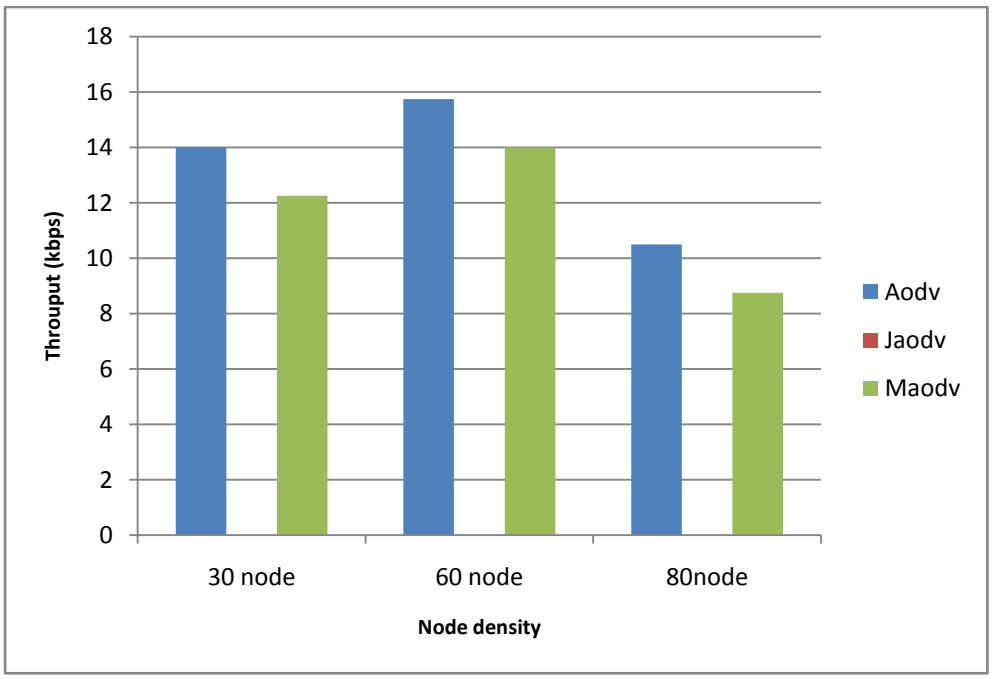

Figure 4: Throughput under AODV, JAODV and MAODV

Analysis of Throughput:

Higher value of throughput ensures large number of data packets successfully received at the Destination node. From the above figure it analyzed that under jamming node attack the Throughput of MAODV is more nearly similar to normal AODV, as compared to JAODV under Jamming node attack. Figure shows with increasing the number of nodes, throughput of network also increases AODV.

V. CONCLUSION

This work carried out the detailed analysis of Jamming attack prevention and its detection through the trust mechanism with AODV routing protocol which is simulated by NS-2 for WSN on the basis of different performance metrics viz. packet delivery ratio, end to end delay, residual energy and average throughput. These performance metrics are analyzed for the AODV, JAODV and MAODV routing protocols by varying the node density for fixed network. Simulation of routing protocols provides the facility to select a good environment for routing and gives the knowledge how to use routing schemes in attack network. Simulation results show that, as the density of nodes increases in the network, the performance of the routing protocols decreases. Attacker nodes affect the performance of routing protocols most as path break increases. According to simulation results as the AODV prevent through the MAODV, the packet delivery ratio, Throughput and End to End delay of routing protocol increases as compare to the detection of AODV through the MAODV compare to JAODV Decreases.

REFERENCES

1. P. Jeyabharathi, A. Sivasankari, M. Maharasi, “An Efficient Security Mechanism for Data Reporting In Wireless Sensor Networks” www.ijera.com Vol. 3, Issue 5, Sep-Oct 2013, pp.333-338
2. Dong-Wook Kim, Wan-Seon Lim, and Young-Joo Suh, "A Multichannel Relay MAC Protocol for IEEE 802.11 Wireless LANs," International Journal of Communication Systems.
3. Tarun Anand Malik , “Target tracking in wireless sensor networks” Maharishi Dayanand University (India) May, 2005
4. Shilpi Agarwal, Rajeshwar Lal Dua and Ravi Gupta, “Performance evaluation of parameters Using DSR Routing Protocol in WSNs” International Journal of Advanced Research in Computer Science and Software Engineering 2 (8), August- 2012, pp. 1-6
5. Devendra Prasad and Reema Goyal “Secure and Energy Efficient Centralized Routing Protocol for Hierarchical WSN” www.ijerd.com Volume 2, Issue 9 (August 2012), PP. 41-45
6. Amer A. Al-Rahayfeh, Muder M. Almi’ani, and Abdelshakour A. Abuzneid, “parameterized affect of transmission-range on lost of network connectivity of wireless sensor networks” International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.3, August 2010

7. Mohsin Raza Jafri, Nadeem Javaid, Akmal Javaid, Zahoor Ali Khan, "Maximizing the Lifetime of Multi-chain PEGASIS using Sink Mobility", Mar 18, 2013
8. Ouadoudi Zytoune1 and Driss Aboutajdine, "A Lifetime Extension Protocol for Data Gathering in Wireless Sensor Networks" , International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 4 No. 3 Nov. 2013, pp. 477-482
9. Samia A. Ali and Shreen K. Refaay, "Chain-Chain Based Routing Protocol", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011
10. Tarun Gulati and sunita Rani, "An improved pegasis protocol to enhance energy utilization in WSN", International Manuscript ID: ISSN2249054X-V2I3M7-052012 VOLUME 2 ISSUE 3 May 2012.
11. Nisha Sarwade, Sanjay Waware and Pallavi Gangurde, "A Review of Power Efficient Hierarchical Routing Protocols in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 2, Mar-Apr 2012.
12. Rathna. R and Sivasubramanian, "Improving energy efficiency in wireless sensor networks through scheduling and routing", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.1, January 2012.
13. Razieh Sheikhpour, Sam Jabbehdari and Ahmad khademzadeh, "A Cluster-Chain based Routing Protocol for Balancing Energy Consumption in Wireless Sensor Networks ", International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 2, April, 2012
14. Se-Jung Lim and Myong-Soon Park, "Research Article Energy-Efficient Chain Formation Algorithm for Data Gathering in Wireless Sensor Networks", International Journal of Distributed Sensor Networks Volume 2012, Article ID 843413, 9 pages doi:10.1155/2012/843413 July 2012
15. Mohammad soleimani, mohammad ghasemzadeh and mehdi agha sarram, "A New cluster based routing protocol for prolonging network lifetime in wireless networks", Middle-East journal of scientific Research7(6) 884-890 2011
16. Ge´rard Chalhoub and Michel Misson, " Cluster-tree based energy efficient protocol for wireless sensor networks", Institute of Electrical and Electronics Engineers, NOV-2010.
17. Young-Long Chen, Jia-Sheng Lin, Yung-Fa Huang, Fu-Kai Cheung and Jen-Yung Lin, "Energy Efficiency of a Chain-Based Scheme with Intra-Grid in Wireless Sensor Networks", 2010 International Symposium on Computer, Communication, Control and Automation,VOL.2, ,2010, pp.484-487.
18. Cong Wang1 and Cuirong Wang, "A Concentric Data Aggregation Model in Wireless Sensor Network ,"PIERS Proceedings, Beijing, China, March 23–27, 2009.