ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Implementation Paper of Packet Hiding Method for Preventing Jamming Attack in Wireless Network

Priya Bhatt [1], Kapil vyas[2]

P.G. Student, Department of Computer Engineering, BM Engineering College & Technology, Indore, India[1]

Assistant Professor, Department of Computer Engineering, BM Engineering College & Technology, Indore, India[2]

ABSTRACT: Wireless network infrastructure (static) & infrastructure less network (dynamic).where jamming attack in possible on infrastructure less network is also known mobile ad-hoc network. Selective jamming attack directly targeting real path in in wireless sensor network. Jamming is address under an external thread model. Selective jamming active short period of time but is targeting message of high importance. It's possible in Transmission control protocol & routing. Selective jamming attack reflection of electromagnetic energy for the purpose of disrupting electronic device or system. due to open nature of infrastructure wireless network it's very difficult & counter in network. but overcome this attack using combining cryptography primitive, analyze the security of our method, evaluate their computational & communication overhead.

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

I. INTRODUCTION

Wireless network is infrastructure less network is depend upon uninterrupted availability of wireless medium. in a wireless network for interconnect participating nodes used wireless medium. in external threat model jamming easily addressed. Where jamming blocking communication in wireless via block path between nodes .open nature of wireless network it's difficult to detect & counter jamming attack. Classification, by combining cryptographic primitives with physical-layer attributes to be proposed. in the physical layer. Where selective jamming attacks in two multi-hop wireless network scenarios. in a first scenario, attacker target a TCP(transmission control protocol) connection establish over a multi- hop wireless route. at the other hand second scenario, the Network-layer control message transmitted ,the jammer targeted attack during route establishment process.

a strong hiding commitment scheme (SHCS) is based on symmetric cryptography which is used to keeping the computation & communication overhead to a minimum. we used strong hiding commitment scheme because of jamming, jamming may be performed intentionally or unintentionally attack the wireless network either stopped or disturbed communication.Noise,collision,interference these are various form of jamming.

II. PROPOSED WORK

A. 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. In a wireless network protocols are classified with different- different parameters. Protocols will be classified as supported their mode of functioning and kind of target applications.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

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

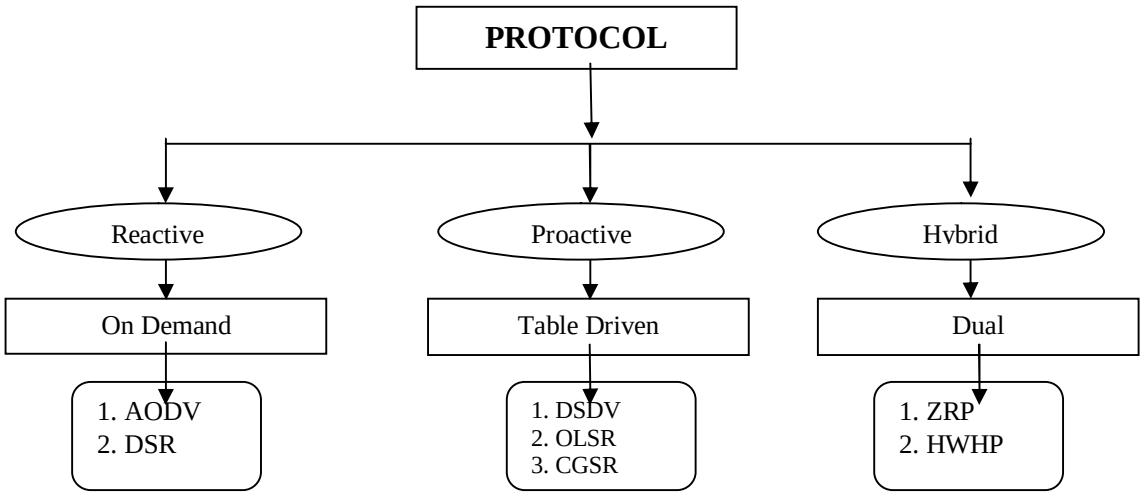


Figure (1): CLASSIFICATION OF PROTOCOL

Where-

a) AODV:-Ad-hoc on demands distance vector routing protocol.
b) DSR:-Destination Source routing protocol.
c) DSDV:-Destination Sequence distance vector routing protocol.
d) OLSR:-Optical link source routing protocol.
e) CGSR:-Cluster head Gateway Switch routing protocol.
f) ZRP:-Zone routing protocol.
g) HWHP:-Hybrid wireless mesh routing protocol.

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 . 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) is an example of a reactive protocol. Adaptive Periodic teen (APTEEN) work like Hybrid protocol incorporates each proactive and reactive idea. They initial compute all routes so improve the routes at the time.

B. AODV (Low Energy adaptive clustering Hierarchy):

AODV may be a self-organizing, adaptive clustering protocol. It uses randomisation for distributing the energy load among the sensors within the network. The 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

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.

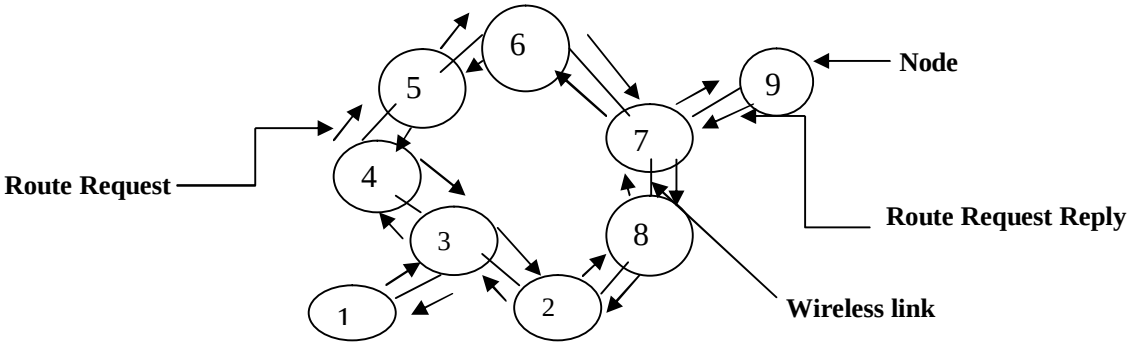


Figure (2): AODV Route Discovery Process

C. 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). There for 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. Its 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 far away from the bs and second level cluster heads are formed almost the b s. 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 verity 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. Thence forth 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).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

III. IMPLEMENTATION

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:

We can easily understand the real world networks via network simulator. The principle idea is that if a system can be modelled, then futures of the model can be changed and the corresponding results can be analysed. Mainly with the help of network simulator we can easily understand system behaviour as well as behaviour of computer network.

OSI LAYER	ATTACKS
Physical Layer	Jamming , Radio interference ,Destruction or Tampering
Application layer	Selective Message Forwarding, Data Aggregation, Clock Skewing.
Data link Collision	Sybil Attack, Interrogation.
Network Layer	Black whole Attack, Wormhole Attack, and Acknowledgement Spoofing.
Transport Layer	De synchronization, Flooding.

Configuring Network simulator

Network simulator is popular software which is support wireless LAN, mobile Ad-hoc network(MANET),wireless sensor network(WSN),Vehicular Ad-hoc network(VANET),Cognitive Radio network, internet of things(IOT),LTE/LTE-Advanced Network. Network simulator is cost effective method for device design and protocol evolution. There were three types of network simulator proprietary and open source network simulator.
where –

- ✓ NS(open source)
- ✓ Net Sim (proprietary software)
- ✓ OPNET(proprietary software)

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

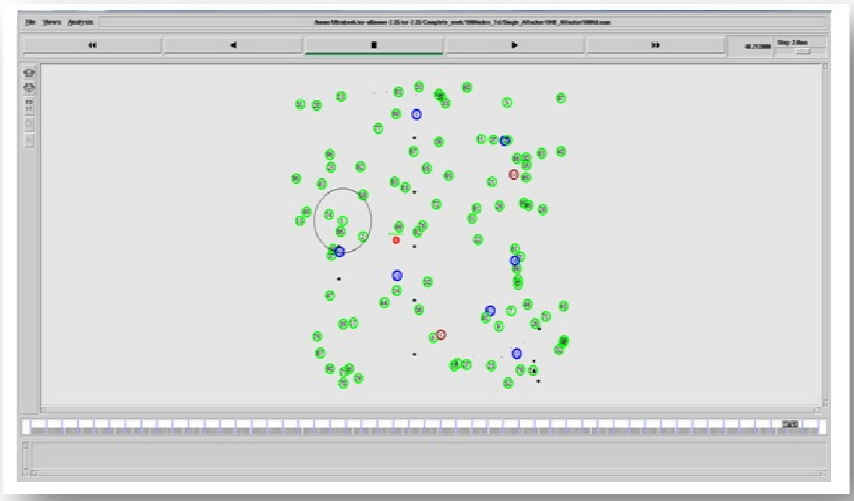
Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Simulation Area(in meter)	2000*2000
Queue type	Drop tail
Channel	Wireless Channel

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

Simulation of Jamming Attack:-



One malicious node in network

We have performed the throughput and delay computation by using network simulator, NS2. In our studies malicious node (which is under hello flood attack) is introduced and performance of network is analyzed with routing protocol. Simulation is performed for no attacker, single attacker, and multiple attacker scenarios. For our network, we have considered 100 nodes. The hello flood attack is simulated by modifying the aodv. h and aodv.cc files in NS2 simulator. There are two types of attacks that are popular with the WSN, namely, physical attack and logical attack. Physical 1ttack includes capturing of the nodes and tampering the nodes, which will lead to loss of data. On the other hand, logical attack includes sinkhole attack, wormhole attack, hello flood attack, selective forwarding attack, Sybil attack, and denial of service attack. in above figure we study jamming attack in wireless network with the help of network simulator we can detect & define malicious node in network.

IV. EXPERIMENTAL RESULT

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

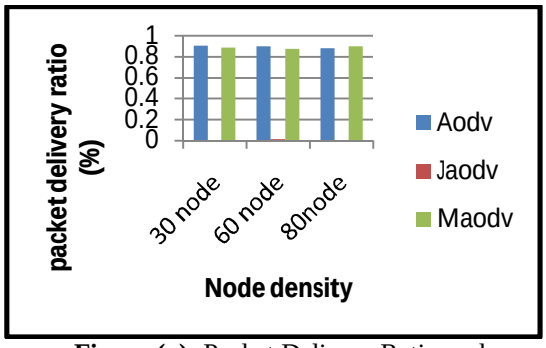


Figure (a): Packet Delivery Ratio under AODV, JAODV and MAODV

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.

B .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. In the time of buffering and processing at intermediate nodes all the delays caused during route acquisition.

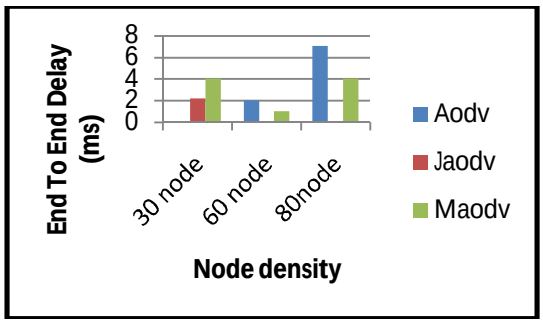


Figure (b): End To End Delay under AODV, JAODV and MAODV

C .Energy:

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

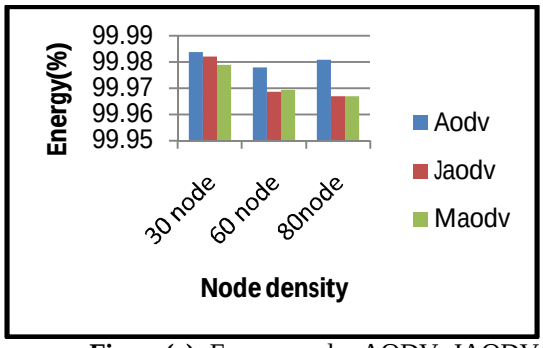
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017



Figure(c): Energy under AODV, JAODV and MAODV

D .Throughput:

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

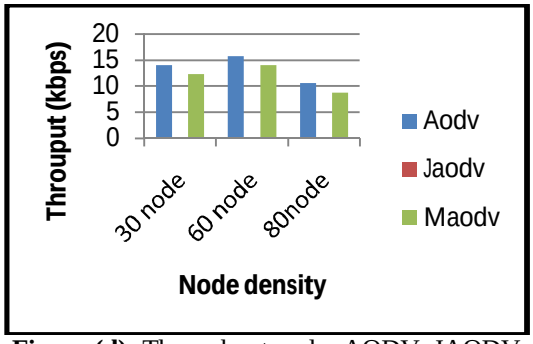


Figure (d): Throughput under AODV, JAODV And MAODV

Analysis of Throughput:
Higher value of throughput ensures large number of data packets successfully received at the Destination node. From the above figure it analysed 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. In routing protocols with the help of simulation we can 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,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

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 Dayan and University (India) May, 2005.
4. Shilpi Agarwal, Rajesh war 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 lots of network connectivity of wireless sensor networks" International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.3, August 2010 .
7. Nadeem Javaid, Akmal Javaid, Mohsin Raza Jafri, 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 "Improving energy efficiency in wireless sensor and routing", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.1, January 2012 .

12 Razieh Sheikh pour, 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.

13. 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.
14. Mohammad Suleiman, Mohammad ghasemzadeh and mehdiaghsarram, "A New cluster based routing protocol for prolonging network lifetime in wireless networks", Middle-East journal of scientific Research7 (6) 884-890 2011.
15. Gerard Calhoun and Michel Misson, "Cluster-tree based energy efficient protocol for wireless sensor networks", Institute of Electrical and Electronics Engineers, NOV-2010.
16. yang-Long Chen, Jia-Sheng Lin, Yung-Fa Huang, Fu-Kai Cheung and Jen-Yung Lin, "Energy Efficiency of 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 Curing Wang, "A Concentric Data Aggregation Model in Wireless Sensor Network ,"PIERS Proceedings, Beijing, China, March 23–27, 2009.