Secure Routing Against DDoS Attack in Wireless Sensor Network

[1]Surendra Nagar, [2]Shyam Singh Rajput , [3]Avadesh Kumar Gupta, [4]Munesh Chandra Trivedi
[1, 2]Dept. of Information & Communication Technology [4]Dept. of Computer Science & Engineering
[1, 2]ABV-IIITM, Gwalior [3]IMS, Ghaziabad [4]ABES Engineering College, Ghaziabad
[1]surendra@iiitm.ac.in, [2]ershyamrajput@gmail.com [4]munesh.trivedi@gmail.com

Abstract— **Wireless sensor network is a low cost network to solve many of the real world problems. These sensor nodes used to deploy in the hostile or unattended areas to sense and monitor the atmospheric situations such as motion, pressure, sound, temperature and vibration etc. The sensor nodes have low energy and low computing power, any security scheme for wireless sensor network must not be computationally complex and it should be efficient. In this paper we introduced a secure routing protocol for WSNs, which is able to prevent the network from DDoS attack. In our methodology we scan the infected nodes using the proposed algorithm and block that node from any further activities in the network. To protect the network we use intrusion prevention scheme, where specific nodes of the network acts as IPS node. These nodes operate in their radio range for the region of the network and scan the neighbors regularly. When the IPS node find a misbehavior node which is involves in frequent message passing other than UDP and TCP messages, IPS node blocks the infected node and also send the information to all genuine sender nodes to change their routes. All simulation work has been done using NS 2.35. After simulation the proposed scheme gives feasible results to protect the network against DDoS attack. The performance parameters have been improved after applying the security mechanism on an infected network.**

Keywords— WSNs, sink node, IPS, DDoS attack, security Algorithm, intrusion;

I. INTRODUCTION

WSN is interesting and emerged as a new area of research to solve many real world problems. WSN consists of devices that have simple circuit, less cost, small size batteries, small memory and processing power etc. [3, 4, 5]. In future the WSNs are assume to be contained of thousands of low cost nodes, every node having more sensing power with limited communication and computational power [1, 2, 9] which gives the freedom to deploy a scalable sensor network. A wireless sensor network consists of many small devices that are able to sense and monitor the environmental conditions such as heat, pressure, vibration; motion, sound etc. depend on the different applications. These sensor networks are deployed in much kind of environments for commercial, civil, and military Applications such as surveillance, forest fire monitoring, vehicle tracking, wild animal tracking, medical, and data gathering. These networks combine wireless communication and minimal computational facilities with sensing of physical phenomenon which can be easily embedded in our physical environment. In disasters situations like hurricanes, earthquakes, tsunami and similar other unfortunate natural disasters wireless sensor networks are very useful for rescue operations in such conditions and give the useful information and monitor these situations regularly.

WSN's are the special case of ad-hoc networks have very less or no mobility. These networks are widely used in recent years for many applications, because they are able to sense and monitor any environment in a reliable way, where a normal human can't able to reach. These networks are data centric. The basic objective of a sensor node is to sense and collect the physical attributes for a particular area, so these nodes should be deployed in such a manner that the each and every point of the given area sense completely sensor nodes should be deployed with accurate density.

Routing of data is a major issue for any network. In sensor networks, routing is performing by many hopes or sensor nodes where the main objective is to transmit the data from source node to base station node (destination node). The base station node is a well known node to all sensor nodes means every sensor node has the information about the location of base station. The base station node has more powerful than a normal sensor node and it may be mobile for mobility based applications or may be static for non mobility applications. To discover the routes and maintain these routes from various situations like node failure is very difficult task in WSN, because of low energy and frequent changes in node position. Thus, the important factors to design a routing protocol are minimum energy consumption [11] and maximum lifetime of the network.

Various routing protocols have been developed to increase the lifetime and energy efficiency in wireless sensor networks. Secure data routing [6, 7] [8, 10] in wireless sensor networks is very typical task, because these networks have limited resources. Due to the deployment of sensor nodes in hostile and unattended environments these networks are vulnerable to network insider as well as outsider attacks. Node capturing and node compromised are the general attacks in these networks. Sensor networks are also sensitive to DDoS attack, black hole attack, gray-hole attack, selective forwarding attack and Sybil attack etc. To design a security mechanism is a very difficult task for WSNs, because a complex and time

978-1-5090-6218-8/17/$31.00 ©2017 IEEE

consuming scheme is not feasible for sensor networks. Our goal is to design a security model, which is simple and feasible and defend the network against DDoS attack. The objective of research is to design a secure routing scheme, which can effectively able to protect the wireless sensor network against DDoS attack and which can deal with the security of data routing in wireless sensor network. To prove the proposed methodology we propagate the DDoS attack in a normal network and second one is to overcome the network from DDoS attack.

The remainder of this paper is organized as follows: Section II introduces related work. Section III describes the proposed methodology. Section IV explains simulation result and discussion, and finally conclusion and future work defined in Section V.

II. RELATED WORK

WSN is very much popular due to the fact that these networks collect the data from unattended and hostile areas. Despite the fact of popularity of WSNs, these networks are very much exposed to attacks. Security is a important factor in any network, so the research is going-on for the security in WSNs to prevent the network from several kind of attacks. Qian et al. [12] proposed a framework which provides two features first is security and second is survivability these both features are very important for several applications in wireless sensor network. They have proposed the security and survivability in one architecture with composite sensor nodes. To explain the co-operation between survivability and security, they also design a key management policy for security in this architecture and analyses this scheme for the proposed framework to provide the security and survivability both together. The results of this scheme shows that how a good design can give better improvement for both the security and survivability in wireless sensor networks, but in some situations the framework is not able to balance in survivability and security, so this is the small drawback of this scheme. To overcome this shortcoming Thein T [13] proposed framework that is able to provide all services when, attacks and failure of network occurs. The framework for survivability and fault tolerance is stands against failure and security problems.

Boukerche et al. [14,16] has described that localization systems can be the possible target of an attack that could compromise the entire functioning of a WSN and lead to incorrect military plans and decision making, among other problems. They shows that how current available localization based systems are vulnerable to many security attacks, and how existing schemes can be used to prevent these attacks in WSNs. For their secure localization system they distribute the system into three components i.e. distance estimation, localization algorithm and position computation. In this article they shown the drawbacks and limitations of current available localization systems and different types of security attack on these systems and not propose any new idea about secure localization system. The data security in WSNs i.e. authentication, confidentiality and integrity is a difficult task because WSN is a large scale network which consists thousands of sensor nodes that are deployed in hostile areas and vulnerable to many attacks. To overcome above security problems and prevent the WSN from different types of network attacks Ren et al. [15] proposed a framework in which secret keys are related to many geographical positions and every node stores a few keys based on its own position. This position-aware scheme effectively bound the impact of compromised nodes only to their local area without affecting the data security. The proposed end-to-end data security and multifunctional key management framework gives both node-to-node and node-to-sink authentication with the forwarding routes report. The given framework is able to prevent the network from DoS attacks. But the scheme is more complex and time consuming due to the cryptographic and MAC based approach. One more approach proposed to find DDoS attack in network, which is localization based algorithm [16].

D Souza et al [23] proposed the digital signature based secure multipath routing protocol in which they used public key based digital signature scheme to provide data integrity, authentication between nodes, but the public key based security in WSN is infeasible due to its complexity. In this paper they propose a cryptographic method to prevent from different types of attacks, but did not represent the results practically. Sensor nodes have some limitation as low computational power and low memory, so any complex and time consuming approach is not feasible to provide security and secure data delivery in the network. To overcome this problem a simple approach that is Di Pietro et al. [17] proposed a deep analysis and investigation of security related problems in wireless sensor networks and give some solutions to provide security against some WSNs attacks.

There are several security approaches against the attacks in WSNs like secure key management, cryptographic algorithms [27], MAC based security [20, 23, 28] etc. and the research is moving on continuously in this field. Many schemes are efficient and perfect, but we have to say that if we want something extra than we have to pay for it. So to make the wireless sensor network secure and to fulfill all the security requirements, several computationally complex and time consuming schemes have been used by many of the researchers, which consume more battery power also. In our approach we use IPS based scheme which is based on secure routing. We patched our security module to existing AOMDV routing protocol and analyses the results using NS 2.35 simulator, which gives satisfactory results against DDoS attack in WSNs.

III. SECURE ROUTING AGAINST DDOS ATTACK IN WSN

Secure data routing and prevent the network from various kind of attacks are the major problems in WSN. Our main objective is to design a security model, which can deal effectively against DDoS attack in wireless sensor networks. To prevent

the sensor network from DDoS attack we propose the security scheme.

A. Proposed Security Mechanism

In proposed methodology we introduce a secure routing protocol for WSNs in which we implement following three security modules:

1. Propagate DDoS attack on a normal network.
2. Overcome the network from attack infection.

In proposed methodology we create a security module to prevent the network from DDoS attack, in which we implement our prevention algorithm on the previously infected network. In the proposed methodology we set some specific nodes as IPS node, the IPS nodes keeps scanning the network for a particular region within its radio range to find the nodes which are involving in unwanted, huge and frequent message passing to the particular node. When IPS node detect the intruder node, it blocks all activities of that node in the network and send the reply request to the genuine nodes, which was requesting to the target node for routing their data.

We proposed two algorithms in our methodology, first algorithm to launch the DDoS attack in the normal scenario and second algorithm to prevent the network from the effect of DDoS attack which are as follows:

1. Algorithm to launch DDoS Attack:

Here we have design DDos attack module, through that module we analyze the effect of denial of service attack under AOMDV protocol, DDoS node spread west full packets into the network and consume the network bandwidth so genuine sender can't sends important data from existing path where DDoS node belongs, through this algorithm we explain about denial of service attack.

ALGORITHM 1: Algorithm to launch DDoS Attack

Step1: Create node = m // DDoS spreader nodes.
Step2: Set normal node = n
Step 3: Set abnormal node = m^{th} node // Last node as DDoS.
Step4: Set total host = 2000 // node number m capable to generate data for transfer 2000 node per second.
Step5: Set packet size = 512 bytes/sec.
Step6: Set ScanPort ; // for sending unwanted packets via DOS node.
Step7: Set **Scanrate** = 1 //default value.
Step8: Smax = Packet size * total host; //total packet transmission/sec.
Step9: β = (**Scanrate***Smax / **abnormal node**); //infected packet sends to all normal nodes.
Step10: Set routing = AOMDV;
Lines of code for this algorithm:

```
RREQ_B ( m, n, rr) // broad cast request
{ if (( rr < = 550) && (next hop > 0))
  { if (node in rr && receives request)
    { node 1 = week node // I belongs to n
      Send (m, 1, β) //  β  is infection parameter
       { node infected by β parameter
          }
      }
      Node unreachable;
  }
  Node out of range;
}
```

2. Algorithm to Prevent N/W from DDoS Attack:

Here we implement an algorithm for DDoS attack prevention by IPS (intrusion prevention system). In this scheme specific nodes selected as IPS node lets node P, which monitor all its neighbor and other nodes in its radio range for their behavior and keep their malicious activities in its routing table, then P scan every routing packet, if P detect any abnormal modification then node P block that particular malicious node after that P inform the genuine sender about this abnormal activity, so the genuine sender alter its route computation method, then sender search for other alternative path and update its table, so it can send the data to destination node using updated secure path.

ALGORITHM 2: Algorithm to Prevent N/W from DDoS Attack

Step1: Generate mobile node **M**;
Step2: Set node **S** as Sender; // **S € M**
Step3: Set node **D** as Destination node**;** // **D € M**
Step4: Select Routing protocol = **AOMDV**;
Step5: Start Simulation time = $\mathbf{t_0}$
Step6: Set radio range = **R**;
Step7: Set node P; // **P € M**, P is IPS node;
Step8: P monitors and store the behavior of all neighbors;
Pseudo code for this step:

```
If (Node N load > Max_Lim load || N not forward packets)
{ P creates table for all Congestion Spreader node N;
    Send ( minimize data rate to node N )
    { if (N change data rate )
      { Exist in Route}
     else
     { Send reply packet to S about node N;
       P blocks node N;  }
    }
 Recompute_path ();
}
Else: establish path is source;
}
```

Step9: Recompute_Path (sender, destination, route-pkt)
Pseudo code for this step:

```
{ If (node m in R || neighbor   == true || node N = false )
  {create route table ();
    Receive route packet destination;  }
  Else:  node out of range or destination unreachable;
```

}
Step10: Send acknowledgement to sender node;
Step11: Sender send data packet through secure path;
Step12: Terminate session;

The given algorithm is suitable to protect network from DDoS attack, because it is very simple and have less time complexity. This mechanism blocks all the misbehavior nodes, which are responsible for the DDoS infection in the network.

IV. Simulation and Result Analysis

We have implemented AOMDV protocol with DDoS attack and with prevention of DDoS attack using NS-2.35 simulator [21, 29]. Simulation parameters used to implement the proposed approach are tabulated in the bellow table I.

TABLE I. Simulation Parameters

Simulator	NS2(v-2.35)
Simulation Time	150s
Transmission Range	100 m
Number of nodes	10 to 150
Area Size	800m x 600m
Protocol	AOMDV
Transmission Range	250m
Maximum Speed	0-20m/s
Application Traffic	CBR
Packet Size	512 bytes
Traffic Rate	4 packet/sec
Node Mobility Model	Random Way-point Model
Pause Time	10, 20, 60, 100 to 140 sec
Mac model	802.15.4

We used the performance parameters i.e. Packet Delivery Ratio (PDR) [20], Average and to End Delay (AE2ED) [20], Normalized Routing Load (NRL) and Packet Loss Percentage (PLP) to compare the performance of proposed methodology and normal AOMDV protocol.

First we deployed a sensor network, which have 150 nodes to simulate the normal behavior and analyze the results based on above parameters. Further we take the same network scenario to launch and propagate the DDoS attack using our proposed algorithm in which we select a node as the intruder node which propagates the attack in the network by sending thousands of message passing request to the target node so it can keep busy the target and prevent it from serving to the genuine node requests. The intruder node infects other nodes also in same manner. When we implement the attack module on the normal scenario, the performance parameters of the network have been degraded tremendously due to the unwanted message overflow on compromised nodes.

In the proposed methodology we provide a security module to prevent the network from DDoS attack, in which we implement our prevention algorithm with the compromised network. In the proposed methodology we set some specific nodes as IPS node, the IPS nodes keeps scanning the network for a particular region within its radio range to find the nodes which are involving in unwanted, huge and frequent message passing to the particular nodes. When IPS node detect the intruder node, it blocks all activities of that node in the network and send the reply request to the genuine nodes, which was requesting to the target node for routing their data.

First we simulate, analyze and compare the performance all three scenarios i.e. Normal-AOMDV, DDoS-AOMDV and Secure-AOMDV in terms of different pause time V/s all four performance parameters (PDF, NRL, E2ED and PLP). Simulation results in Figure I, II, III and IV shows that the PDF, NRL, E2ED and PLP are degraded for DDoS-AOMDV because this particular scenario is infected by DDoS attack. The performance is increasing with the pause time. Here when we increase the pause time means that we decreasing the mobility of sensor nodes. For Secure-AOMDV scenario, we can see that the performance is increases approximate to the Normal-AOMDV.

Now we compare the number of nodes V/s all four performance parameters (PDF, NRL, E2ED and PLP) shown in Figure V, VI, VII and VIII. In the graphs we can see that performance is decreasing as we increase the Number of nodes. When we increase the Number of Nodes means we increase the connection between the sensor nodes and for DDoS-AOMDV, we increase the malicious nodes also. For Secure-AOMDV scenario, we can see that the performance is increases approximate to the Normal-AOMDV.

V. Conclusion

In this paper we have propose a security scheme for WSNs, which is able to defense the network from DDoS attack. We have compared the performance of three scenarios then analyze the results. As we can see the performance comparison between Normal-AOMDV, DDoS-AOMDV and Secure-AOMDV, our security mechanism is working properly for AOMDV and it prevent the network from DDoS attack by blocking the intruder nodes. The performance in our scenario is improved as compare to attack scenario and it is approximately approaching to the normal scenario. The performance of routing protocol is improved in the existing DDoS attack.

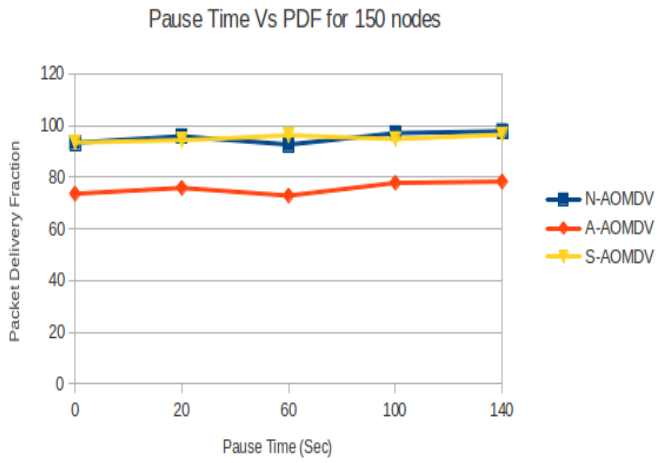

Figure I: Pause Time Vs Packet Delivery Fraction

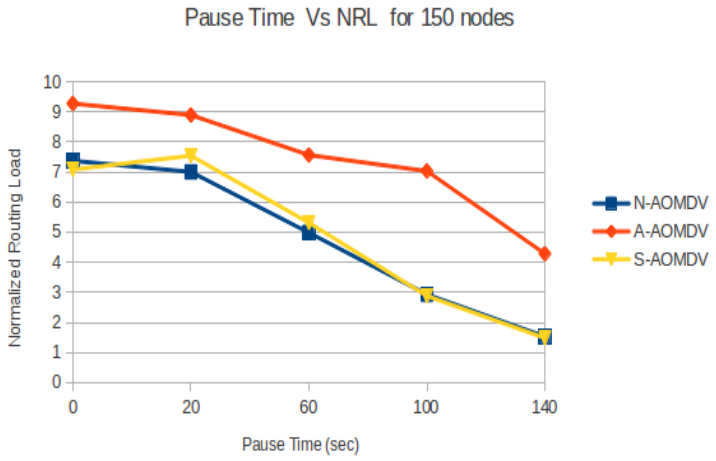

Figure II: Pause Time Vs Normalized Routing Load

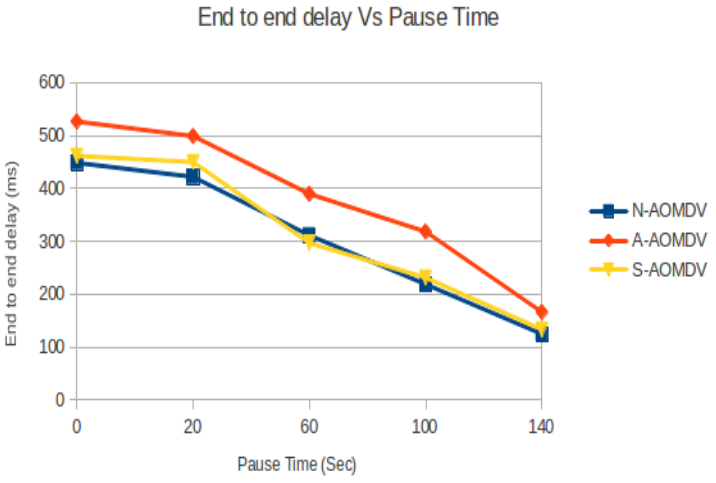

Figure III: Pause Time Vs End to End Delay

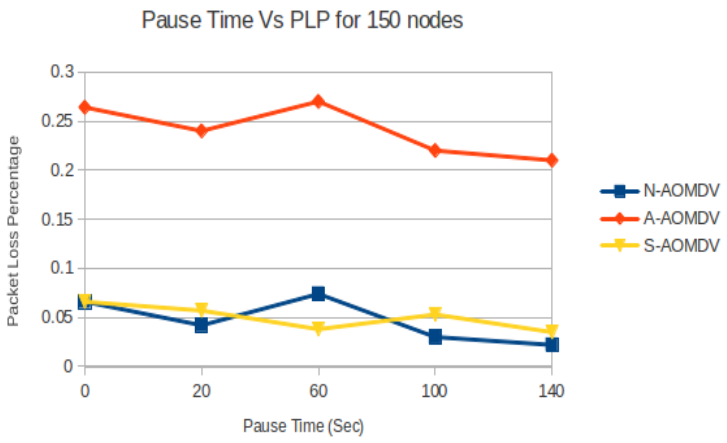

Figure IV: Pause Time Vs Packet Loss Percentage

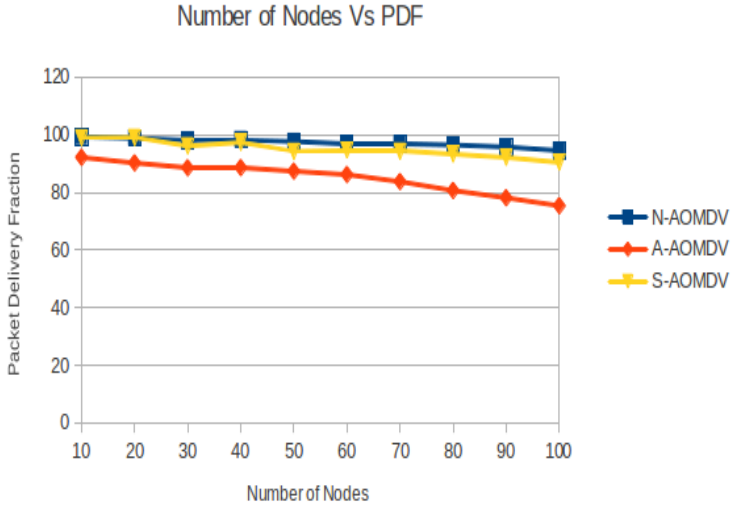

Figure V: Number of Nodes Vs Packet Delivery Fraction

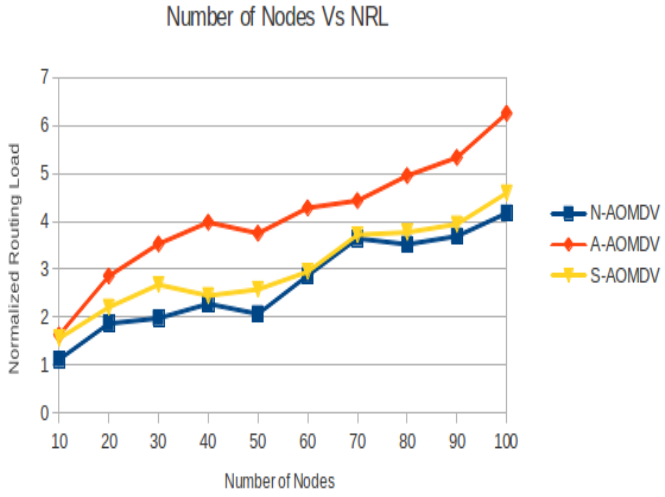

Figure VI: Number of Nodes Vs Normalized Routing Load

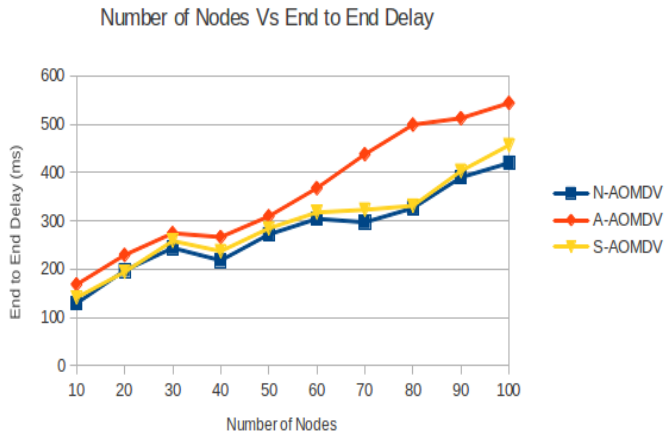

Figure VII: Number of Nodes Vs End to End Delay

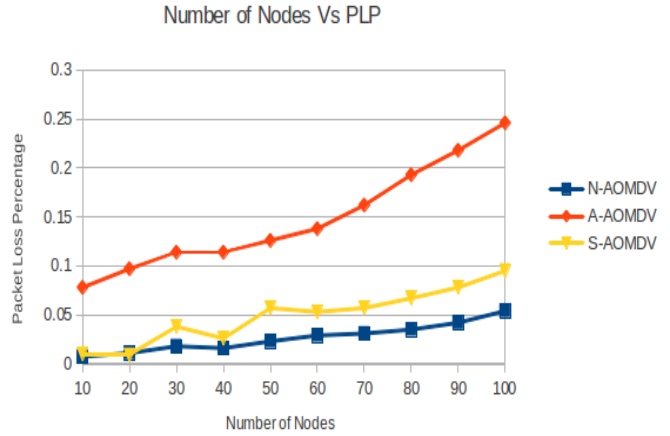

Figure VIII: Number of Nodes Vs Packet Loss Percentage

VI. REFERENCES

[1] C. D. M. Cordeiro and D. P. Agrawal, Ad hoc and sensor networks: theory and applications. World Scientific, 2011.

[2] D. G. Padmavathi, M. Shanmugapriya, et al., "A survey of attacks, security mechanisms and challenges in wireless sensor networks," (IJCSIS) International Journal of Computer Science and Information Security, vol. 4, no. 2, pp. 211-219, 2009.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor-networks, " Communications magazine, IEEE, vol. 40, no. 8, pp. 102-114, 2002.

[4] C. Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities,a nd challenges," Proceedings of the IEEE, vol. 91, no. 8, pp. 1247-1256, 2003.

[5] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks research challenges," Ad hoc networks, vol. 2, no. 4, pp. 351-367, 2004

[6] M. Khan, B. Bhargava, S. Agarwal, and L. Lilien, "Self configuring node clusters, data aggregation, and security in microsensor networks, 2002.

[7] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks,"Communications of the ACM, vol. 47, no. 6, pp. 53-57, 2004.

[8] H. C¸ am, S. Ozdemir, P. Nair, D. Muthuavinashiappan, and H. Ozgur Sanli,"Energy-efficient secure pattern based data aggregation for wireless sensor networks," Computer Communications, vol. 29, no. 4, pp. 446-455, 2006.

[9] L. Butty´an, D. Gessner, A. Hessler, and P. Langendoerfer, "Application of wireless sensor networks in critical infrastructure protection: challenges and design options in emerging wireless networks," Wireless Communications, IEEE, vol. 17, no. 5, pp. 44-49, 2010.

[10] F. Wang and J. Liu, "Networked wireless sensor data collection: Issues, challenges, and approaches," Communications Surveys & Tutorials, IEEE, vol. 13, no. 4, pp. 673-687, 2011.

[11] W. Ding, S. Iyengar, R. Kannan, and W. Rummler, "Energy equivalence routing in wireless sensor networks," Microprocessors and Microsystems, vol. 28, no. 8, pp. 467-475, 2004.

[12] Y. Qian, K. Lu, and D. Tipper, "A design for secure and survivable wireless sensor networks," Wireless Communications, IEEE, vol. 14, no. 5, pp. 30-37, 2007.

[13] T. Thein, S. M. Lee, and J. S. Park, "Improved method for secure and survivable wireless sensor networks," in proceedings Computer Modelling and Simulation UKSIM'09. 11th IEEE International Conference on Sens or Networks, pp.605-610, 2009.

[14] A. Boukerche, H. Oliveira, E. F. Nakamura, and A. A. Loureiro, "Secure localization algorithms for wireless sensor networks," Communications Magazine ,IEEE, vol.46,no. 4, pp. 96-101, 2008.

[15] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks," Mobile Computing, IEEE transactions on, vol. 7, no. 5, pp. 585-598, 2008.

[16] O. Demir and B. Khan, "Finding ddos attack sources: Searchlight localization algorithm for network tomography," 7thIEEE International on IWCMC, WirelessCommunication, pp. 418-423, 2011.

[17] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Data security in unattended wireless sensor networks," Computers, IEEE Transactions on, vol. 58, no. 11, pp. 1500-1511, 2009.

[18] H. Wen, J. Luo, and L. Zhou, "Lightweight and effective detection schemefornodeclone attack in wireless sensor networks," IET wireless sensorsystems, vol.1, no.3, pp. 137-143, 2011.

[19] J. Chen, "Broadcast authentication protocol scheme based on dbp-msp and safe routing in wsn against ddos attacks," in proceedings Networkingand Distributed Computing (ICNDC), 2011 2nd IEEE International Conference on wireless networks, pp. 170-174, 2011.

[20] K. V Arya and S. S. Rajput, "Securing AODV routing protocol in MANET using NMAC with HBKS Technique," IEEE International Conference on SPIN, pp. 281-285, Feb 2014.

[21] S. S. Rajput, V. Kumar and K. Dubey, "Comparative Analysis of AODV and AODV-DOR routing protocol in MANET " International Journal of Computer Application, vol. 63, no. 22, pp. 19-24, Feb 2013

[22] S. Jokhio, I. Jokhio, and A. Kemp, "Node capture attack detection and defence in wireless sensor networks," Wireless Sensor Systems, IET, vol.2, no.3, pp.161-169, 2012.

[23] R. D'Souza, G. Varaprasad, et al., "Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks," Sensors Journal IEEE, vol. 12, no. 10, pp. 2941-2949, 2012.

[24] A. Sahana and I. S. Misra, "Implementation of rsa security protocol for sensor network security: Design and network lifetime analysis," 2nd IEEE International Conference on Wireless VITA, Wireless Communication, pp. 1-5, 2011.

[25] M. Das, "Two-factor user authentication in wireless sensor networks,"Wireless Communications, IEEE Transactions on, vol. 8, no. 3, pp. 1086-1090, 2009.

[26] Y. Liu, J. Li, and M. Guizani, "Pkc based broadcast authentication using signature amortization for wsns," Wireless Communications, IEEE Transactionson, vol.11, no. 6, pp. 2106-2115, 2012.

[27] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography,"IEEE International Conference on Wireless Sensor Networks, pp. 1-6, 2010.

[28] S. S. Rajput and M. C. Trivedi, "Securing ZRP routing protocol in MANET using Authentication Technique," IEEE International Conference on CICN, pp. 872-877, Nov. 2014

[29] N. Sharma, A Gupta, SS Rajput and V. Yadav, " Congestion Control Technique in MANET: A Survey " 2nd IEEE International Conference on CICT, pp. 280-282, Feb. 2016.