PERFORMANCE EVALUATION OF WIRELESS SENSOR NETWORK UNDER HELLO FLOOD ATTACK

Mohammad Abdus Salam and Nayana Halemani

Department of Computer Science, Southern University and A&M College
Baton Rouge, USA

ABSTRACT

Wireless sensor network (WSN) is highly used in many fields. The network consists of tiny lightweight sensor nodes and is largely used to scan or detect or monitor environments. Since these sensor nodes are tiny and lightweight, they put some limitations on resources such as usage of power, processing given task, radio frequency range. These limitations allow network vulnerable to many different types of attacks such as hello flood attack, black hole, Sybil attack, sinkhole, and many more. Among these attacks, hello flood is one of the most important attacks. In this paper,we have analyzed the performance of hello flood attack and compared the network performance as number of attackers increases. Network performance is evaluated by modifying the ad-hoc on demand distance vector (AODV) routing protocol by using NS2 simulator. It has been tested under different scenarios like no attacker, single attacker, and multiple attackers to know how the network performance changes. The simulation results show that as the number of attackers increases the performance in terms of throughput and delay changes.

KEYWORDS

Wireless sensor networks, security, hello flood attack, passive attack, active attack

1. INTRODUCTION

Applications of WSN are numerous and growing rapidly. WSNs are widely used in situations like battlefield, intelligent communications, smart buildings, bushfire response, military command, wildlife monitoring, industrial quality control, observation of critical infrastructures, examining human heart rates, smart homes, and many more scenarios. Wireless sensor networks are prone to failures and malicious attacks. Due to their deployment in remote areas, these networks may lead to numerous security threats and affect network performance. Many researchers have discussed these various types of attacks and security issues [1-2].

Hello flood attack is most common attack in WSN. In this kind of attack a malicious node keep sending hello request to the legitimate node, which will alter the security of the system [4].It occurs on network layer in which an adversary node, which is not a legal node,sends hello packets request to most of the nodes in the network. As these adversary nodes have high transmission power, they have capacity to transmit hello packets to most nodes in network and become reason to break security of WSN, which in turn lead to bad network performance. Although there are many detection and prevention algorithms, but most of the algorithms have some disadvantage by which they fail to detect attacker in network.

In many cases the hello packets are sent to every node before sending actual packet to know if it is friend or stranger node, if node replies back for hello message then it is considered as friend nodes or otherwise it is stranger node. In some other algorithms if node does not reply in certain threshold time it is detected as malicious node. Hello flood attack can cause harm to the following

DOI : 10.5121/ijcnc.2016.8207

protocols: TinyOs beaconing, directed diffusion and its multipath variant, minimum cost forwarding, clustering based protocols (LEACH, TEEN, PEGASIS), and energy conserving topology maintenance (SPAN, GAF, ECE, AFECA) [3].

In this research, we have considered hello flood attack and identified performance penalties by several metrics such as throughput and delay in networks with no attacker, single attacker, and multiple attackers' scenarios.

The network with no attacker performs well as compared to single and multiple attackers. Network performance of each is evaluated by comparing metrics, which are throughput and delay. Thus it will be able to know by how much percent each case vary and accordingly it may lead to further research for providing good mechanism for detection of attackers and securing the network from attackers.

2. SECURITY GOALS OF SENSOR NETWORK

Many applications rely on security performance of the network. Major security goals of sensor network are as follows [4-8]:

1. DATA CONFIDENTIALITY - Data confidentiality is managing access of files either in storage or in transit. Basically it is the ability to protect messages from attackers so that any message communicated through sensor network remains confidential.
2. DATA INTEGRITY - Data Integrity in sensor networks is needed to ensure the reliability of data and refers to the ability to confirm that the information is not changed due to malicious intent or by accident.
3. DATA AUTHENTICATION **-** The receiving node need to ensure that the data originates from the reliable resource. Due to the wireless nature of the media and the unattended nature of sensor networks, attaining authentication is major challenge.
4. DATA AVAILABILITY – Sensor node may run out of battery power due to large amount of processing or communication and become unavailable, which will cause failure of base station and worsen the entire network. Hence ability of sensor node to use resources or the ability of network for message to communicate determines data availability.
5. DATA FRESHNESS – Data freshness can be attained by ensuring no old data is replayed.
6. SELF-ORGANIZATION – There is no fixed infrastructure for WSN network management hence every sensor node must have capability of self-organizing.
7. TIME SYNCHRONIZATION – Sometimes nodes need to recharge after they have used their power hence it is necessary for nodes to turn off periodically to regain their energy.
8. SECURE LOCALIZATION– Sensor network need accurate location for secured data processing however attacker can easily inject false data in secured location by reporting false signal strengths and my divert communication path.

3. TYPES OF ATTACKERS

Due to the broadcast nature of the transmission medium WSNs are more prone to security attack. Often, nodes are placed in a hostile or dangerous environment where there is no physical protection; hence this may lead to security threats. Many types of attacks were documented. Two major types of attacks are active attack and passive attack. Figure 1 shows the basic classification of attacks under general categories [2].

PASSIVE ATTACKS: A malicious unauthorized node is monitoring and listening to the communication channel. This type of attack is harder to detect since the attacker does not contribute anything in the communication channel. The attacker's intention is to gather confidential information and prepare for an active attack.

ACTIVE ATTACKS: A malicious unauthorized node is monitoring, listening, and modifying the data stream to the communication channel. In this type of attack, the attacker plays an active role and pretends as a valid node. It injects or modifies transmission messages. It may cause denial of services.

Many routing protocols for wireless sensor networks are very simple and very easy to attack. Most of the routing attacks are: hello flood, Sybil attack, wormhole attack, Black hole attack, and selective forwarding attack. Some attacks manipulate the user data directly and some attacks affect the routing protocols.

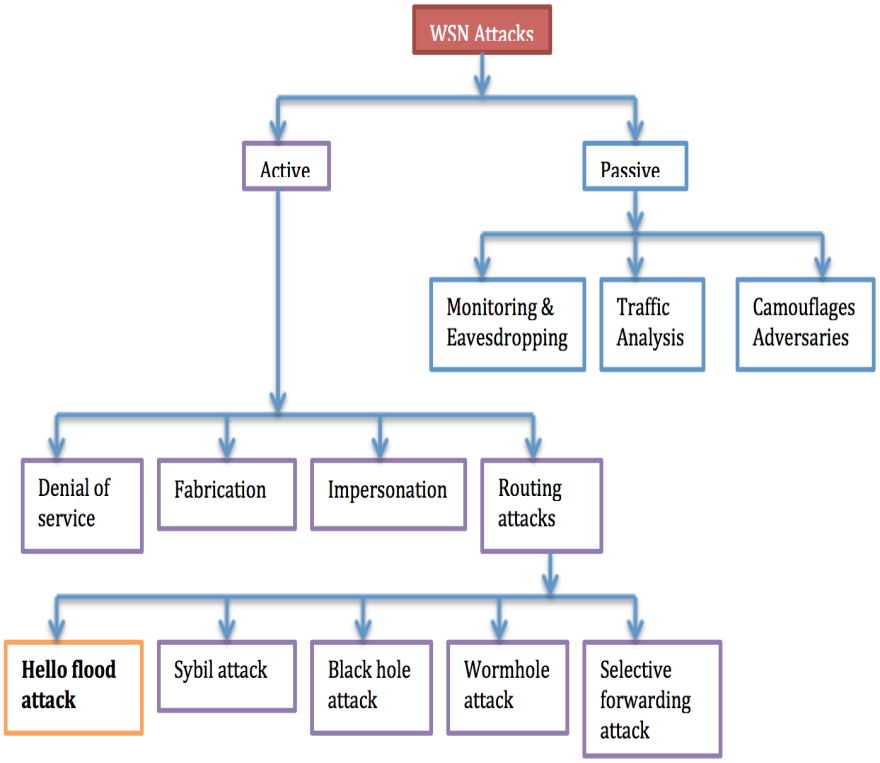

Figure 1: Classification of WSN attacks

Hello flood attack: In WSN, many protocols require to send hello packets to its neighbor. Hello flood attacks make use of such type of packets. This ideal characteristicof the attacker possesses high energy at all time. With this high energy, it has the capacity to send or reply hello packets to another node, which may have been located far away. This may lead to misguidance to neighboring nodes. As a result, the nodes try to send packets through the attacker or it is possible that they may consider it as base station and thus are deceived by the attacker [3]. In the following Figures 2(a) through Figure 2(d), we explain how hello flood attack takes place. Figure 2(a) and Figure 2(b) show no influence of hello flood attacker. The base station sends initial network setup message to the nodes and forms the network (Figure 2(a)). Once the initial setup

phase is completed, the nodes send message to the base station directly or through other intermediary nodes depending upon the network routing topology (Figure 2(a)). A high power adversary node in introduced in the network as an attacker (Figure 2(c)). She is trying to get control of the nodes by sending high power hello messages to the nodes. The legitimate nodes consider the attacker as a valid node or base station and start sending or routing packages through the attacker (Figure 2(d)). Therefore, under the worst-case scenario, the network will be under the full control of the hello flood attacker. Here the attacker sends single-hop broadcast messages to most nodes.

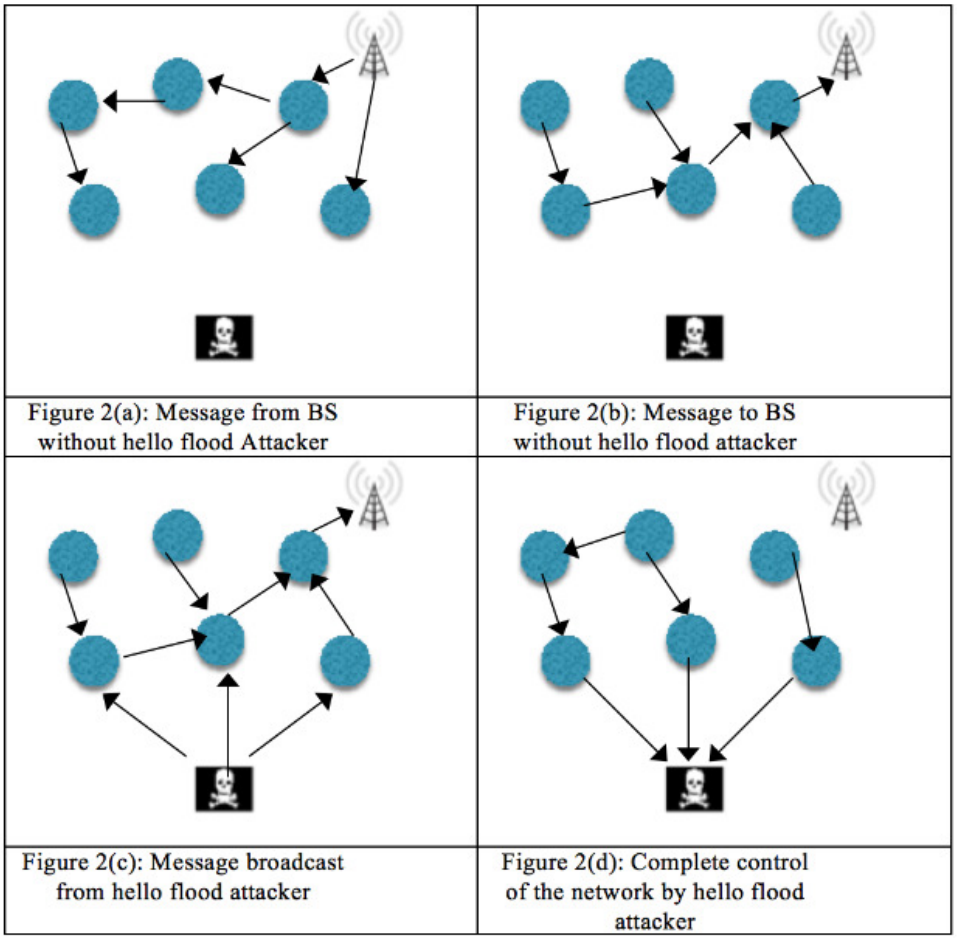

Figure 2(a): Message from BS without hello flood Attacker

Figure 2(b): Message to BS without hello flood attacker

Figure 2(c): Message broadcast from hello flood attacker

Figure 2(d): Complete control of the network by hello flood attacker

Many hierarchical based clustering protocols, such as LEACH and directed diffusion are easy to fall under this type of attack. Many security measurements are proposed to handle the hello flood attack [3].

4. DETECTION & PREVENTION MECHANISM AGAINST HELLO FLOOD

Even though there are different mechanisms to detect and prevent network from this type of attack, there is no such mechanism that is 100% efficient.Adversaries can attack on network flow, network latency, and get control over the networks.Prevention mechanism used in [9] involves authentication between communicating nodes, each node in this is capable of calculating pairwise key between nodes so that network will have secured communication on multi-hop routing. This mechanism is a very secure communication but calculating pairwise key and setting up the route

may need more processing hence this is not efficient. In [14], the author has adopted identity verification protocol and this protocol used echo back mechanism for verification of bi-directional of a link. The attacker can compromise a node before feedback message can block other nodes by dropping feedback messages. Thus when an attacker has high sensitive receiver and powerful transmitter this mechanism becomes inefficient. In [10], the authors used cryptographic method to prevent hello flood attack. In their study, the message reached to destination node can decrypt and verify the message. This mechanism is not efficient when attacker is capable of spoofing its identity and then generates attack. There are many other mechanisms to detect and prevent but every mechanism has been shown inconsistency with regard to security issue and has greater impact on network performance [11].

5. PERFORMANCE FACTOR

As shown in Figure 2, performance of network depends on factors like network delay, success rate, throughput, energy consumption, latency, and network lifetime [6]. These factors are briefly described as follows.

- NETWORK DELAY: It is the measurement of time taken to send the message and time take to successfully receive message at destination.
- ENERGY CONSUMPTION: It is sum of energy used for communication including, energy transmitted (Pt), energy received (Pr), and energy used at idle state (Pi). Assuming each transmission consume an energy unit. Total energy consumption is the total number of packet sent in network.
- SUCCESS RATE: It measures the success rate of message received. It is defined as total number of packetsreceived at destination against total number of packet sent from the sources [10].
- LATENCY: It is the amount of time between start of disseminating a data and its arrival at node interested in receiving the data. Hence latency calculates the performance of individual message.
- THROUGHPUT: It is the measure of packets received per second at the destination
- NETWORK LIFETIME: It is time until message loss rate is above given threshold Packet generation ratio: number of packets that the sensor node transmits in one time period, usually a second [10].

The threats against WSNs can be implemented in different layers of the OSI protocol stack. The common types of these attacks [12], classified based on the OSI layers, are presented in Table 1.

Table 1: WSN attacks on OSI layers

OSI LAYER	ATTACKS
Application Layer	Clock Skewing, Selective Message Forwarding, Data Aggregation Distortion.
Physical layer	Jamming, Radio interference, Tampering or Destruction.
Data link Collision	Exhaustion, Unfairness, Interrogation, Sybil Attack.
Network Layer	Sinkhole, Flooding(Hello flood, Ping flood), Node capture, Selective forwarding or Black hole or Neglect and Greed Sensor nodes Attack,Attack, Wormhole, Spoofed or Altered, Replayed routing information, Acknowledgment spoofing, Misdirection, Internet Smurf, and Homing.
Transport Layer	Flooding (SYN flood), Desynchronization.

6. CONFIGURING NETWORK SIMULATOR

In NS2 simulator, manysensor nodes can be created and data transfer among the nodes is very convenient.After creating the nodes, a connection must be established between the nodes in the network. There are several protocols that can be used to establish connectivity among the nodes. The user datagram protocol (UDP) is a connection less protocol and it can be used when there is a lot of traffic in the system. Transmission control protocol (TCP) is a connection-oriented protocol that provides acknowledgement from the receiver. Once connection is established, data can be sent bidirectional. There are TCP agent and TCP sink. TCP agent is responsible for sending the packets in the network, which can be called as a source node. TCP sink is the receiver node, which receives the packets sent by the sender.

The hello flood attackis introduced into the system by making some of the nodes as malicious nodes. In our system, the simulation is shown from no attacks to multiple attacks.

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 [15].

There are two types of attacks that are popular with the WSN, namely, physical attack and logical attack [13]. 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.

6.1 Simulation Of Hello Flood Attack

In hello flood attack, the node, which receives a message, assumes that the sender has sent it, which is not the case always. It can occur when there is huge amount of traffic in the system. Several cryptographic techniques and methods have been implemented in order to prevent this attack but each one had its own drawback. This attack is simulated in order to create hello flood attack where we can see the target node being flooded by the packets. The aodv.h and aodv.cc contain all the codes about the routing, providing a path for routing and information on the packet forwarding. Figure 3shows the simulation of hello flood attack. A node is made as a target node and it is flooded with lots of hello messages, which creates black circles in the simulator. The user can enter the source and destination as he wishes which is shown in Figure 3. Here, blue nodes are source and destination.Trace file for network having single hello flood attacker is shown in Figure 4.

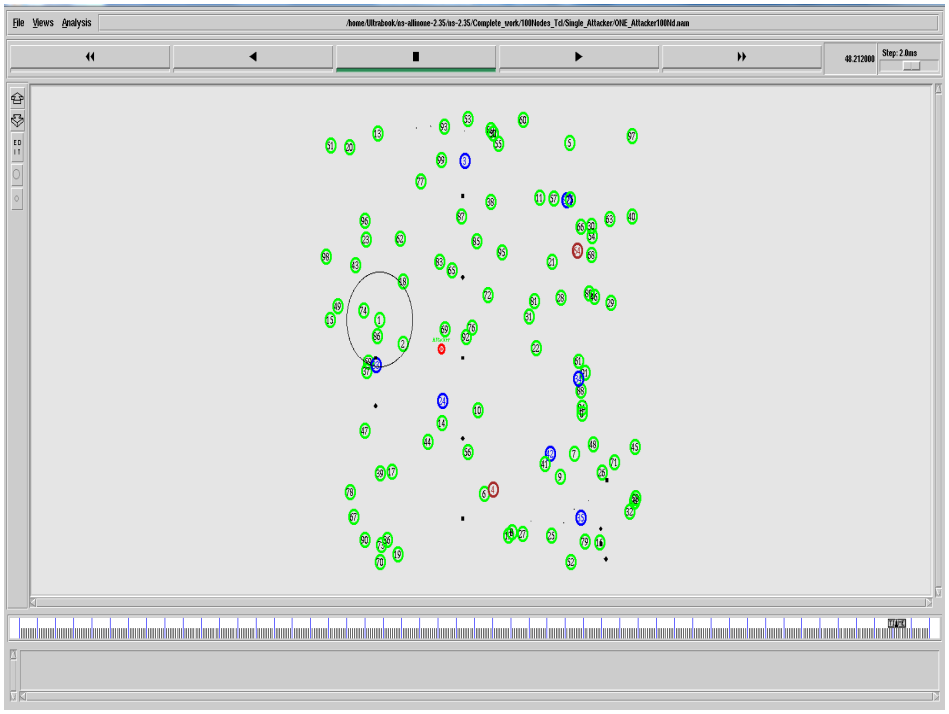

Figure 3: Network with one malicious node(node 100)

Figure 5 and Figure 6 show the network diagrams for 4 and 6 attackers, respectively.

```
s 0.000000000 _0_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [0:255 -1:255 1 0] [0x1 1 [0 2] 4.000000]
s 0.000000000 _1_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [1:255 -1:255 1 0] [0x1 1 [1 2] 4.000000]
s 0.000000000 _2_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [2:255 -1:255 1 0] [0x1 1 [2 2] 4.000000]
s 0.000000000 _3_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [3:255 -1:255 1 0] [0x1 1 [3 2] 4.000000]
s 0.000000000 _4_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [4:255 -1:255 1 0] [0x1 1 [4 2] 4.000000]
s 0.000000000 _5_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [5:255 -1:255 1 0] [0x1 1 [5 2] 4.000000]
s 0.000000000 _6_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [6:255 -1:255 1 0] [0x1 1 [6 2] 4.000000]
s 0.000000000 _7_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [7:255 -1:255 1 0] [0x1 1 [7 2] 4.000000]
s 0.000000000 _8_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [8:255 -1:255 1 0] [0x1 1 [8 2] 4.000000]
s 0.000000000 _9_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [9:255 -1:255 1 0] [0x1 1 [9 2] 4.000000]
s 0.000000000 _10_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 1 0] [0x1 1 [10 2] 4.000
s 0.000000000 _11_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [11:255 -1:255 1 0] [0x1 1 [11 2] 4.000
s 0.000000000 _12_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [12:255 -1:255 1 0] [0x1 1 [12 2] 4.000
s 0.000000000 _13_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [13:255 -1:255 1 0] [0x1 1 [13 2] 4.000
s 0.000000000 _14_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [14:255 -1:255 1 0] [0x1 1 [14 2] 4.000
s 0.000000000 _15_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [15:255 -1:255 1 0] [0x1 1 [15 2] 4.000
s 0.000000000 _16_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [16:255 -1:255 1 0] [0x1 1 [16 2] 4.000
s 0.000000000 _17_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [17:255 -1:255 1 0] [0x1 1 [17 2] 4.000
s 0.000000000 _18_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [18:255 -1:255 1 0] [0x1 1 [18 2] 4.000
s 0.000000000 _19_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [19:255 -1:255 1 0] [0x1 1 [19 2] 4.000
s 0.000000000 _20_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [20:255 -1:255 1 0] [0x1 1 [20 2] 4.000
s 0.000000000 _21_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [21:255 -1:255 1 0] [0x1 1 [21 2] 4.000
s 0.000000000 _22_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [22:255 -1:255 1 0] [0x1 1 [22 2] 4.000
s 0.000000000 _23_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [23:255 -1:255 1 0] [0x1 1 [23 2] 4.000
s 0.000000000 _24_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [24:255 -1:255 1 0] [0x1 1 [24 2] 4.000
s 0.000000000 _25_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [25:255 -1:255 1 0] [0x1 1 [25 2] 4.000
s 0.000000000 _26_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [26:255 -1:255 1 0] [0x1 1 [26 2] 4.000
s 0.000000000 _27_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [27:255 -1:255 1 0] [0x1 1 [27 2] 4.000
s 0.000000000 _28_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [28:255 -1:255 1 0] [0x1 1 [28 2] 4.000
s 0.000000000 _29_ RTR  --- 0 AODV 44 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [29:255 -1:255 1 0] [0x1 1 [29 2] 4.000
```

Figure 4:Trace file for network having single hello flood attacker

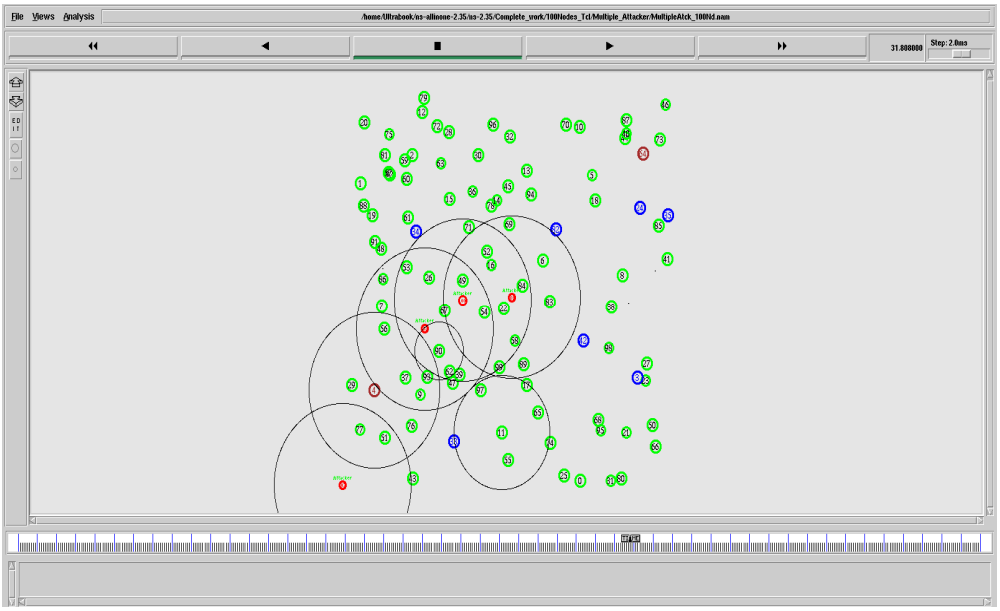

Figure 5: Network with four malicious nodes (100, 101,102, and 103)

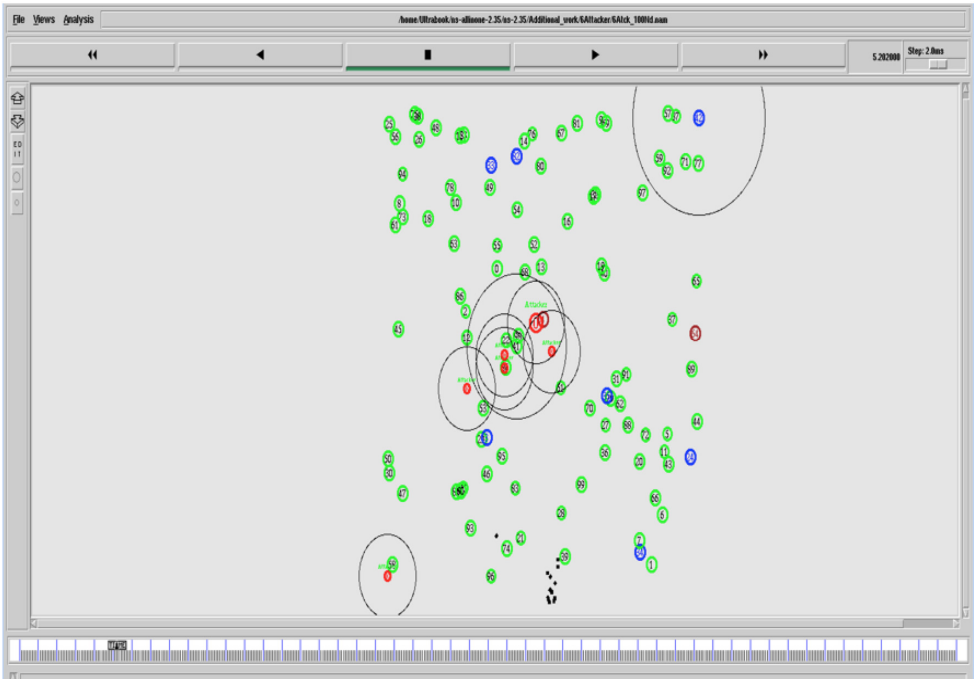

Figure 6: Network with 6 malicious nodes (100,101,102,103,104, and 105)

7. RESULTS

Using the network simulator NS2, the attacks is simulated and graphsare generated to monitor the network performance. It calculates throughput and delay of the network in each case.

Throughput in the network can be affected by various numbers of factors. It plays vital role in analyzing the network performance. The trace file generated is passed as an input in order to generate a graph. The X- axis represents time and Y-axis represents throughput rate. Initially, when transmission starts there is huge amount of traffic in the system, so the throughput is high and slowly it drops as the number of attackers increased (Figure 7).

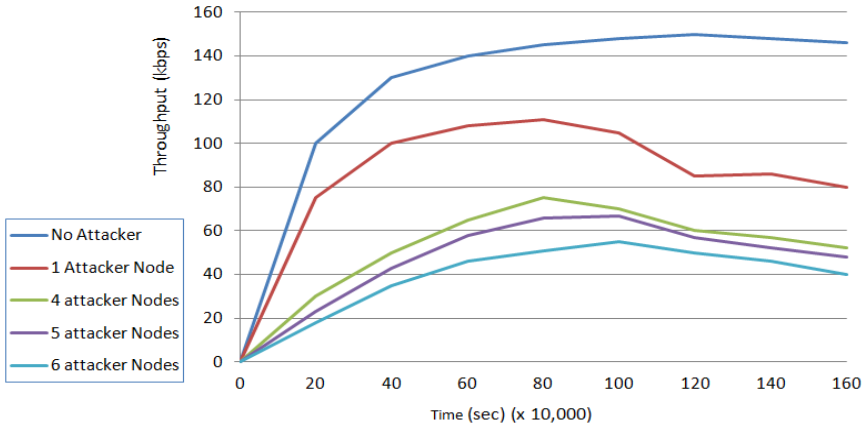

Figure 7:Graph for throughput

The delay is the difference of time between when the message is sent and when it is successfully received at the destination. Like throughput, delay is also one of the factors for analyzing the network performance. In Figure 8, the X-axis represents time and Y-axis represents delay. It shows the effect of delay on the wireless sensor network. Initially, there will not be any delay in network but as time elapses and the number of attackers increase, the delay increases.

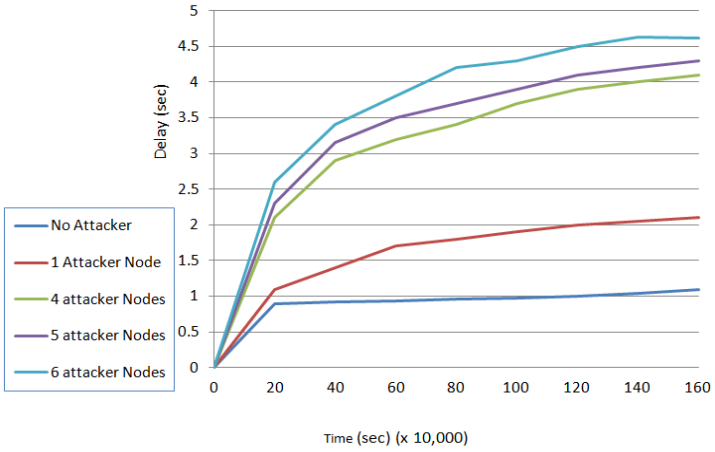

Figure 8: Graph for delay

The Table 2 shows the percentage of increase and decrease in delay and throughput as compared to with no attacker.

Table 2: Simulation output for delay and throughput

Number of Attacker	Delay (in percent)	Throughput (in percent)
1	90.91	44.83
4	272.73	60.07
5	290.91	65.52
6	318.18	72.41

8. CONCLUSION

In this paper, we have simulated hello flood attack using NS2 simulator and performance of network is analyzed based on AODV routing protocol. We have considered 100 sensor nodes. We simulated the network from no attacker scenario to many attackers scenarios. Hello flooding basically occurs when any malicious node in the network transmits packets with very high power in a frequent interval of time. So, the actual damage in the network is based on this periodicity of sending information and power. It does not depend on packet size. The throughput and delay of the network with no attacker and single attacker has no much difference till the first 20 seconds and as number of attackers increases the throughput will decrease and delay increases.

We have considered only delay and throughput as a performance factors. There are other factors or network parameters like latency, success rate, network lifetime, which are not included in this research. As a future exploration, we plan to conduct research on the overall performance of wireless sensor networks on these parameters. Also, there are several research topics on severity of various attacks and their performance measure.

ACKNOWLEDGEMENTS

The authors would like to thank anonymous reviewers for their valuable comments and suggestions that have improved this paper.

REFERENCES

[1] Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, International conference on Advanced Computing Technologies, page: 1043-1045, 2006.

[2] G.Padmavati and D.Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, vol.4, 2009.

[3] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), page: 299-302, 2003.

[4] A. Patham, Hyung-Woo Lee,ChoongSeon Hong, “Security in Wireless Sensor Networks: Issues and Challenges” Advanced Communication Technology (ICACT), 2006.

[5] T. Zia andA. Zomaya, “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC), 2006.

[6] MD.Abdul Hamid,Mamun-Or-Rashid, and ChoongSeon Hong, ”Defense against laptop class attacker in wireless sensor network,” 8th International conference,2006.

[7] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah, and KashifNaseer Qureshi "Security Issue in Attackers in Wireless Sensor Networks", IDOSI Publications, 2014.

[8] J. Undercoffer,S. Avancha, A. Joshi, and J. Pinkston, “Security for Sensor Networks”. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, 2002.

[9] VenkataGiruka,MukeshSinghal,James Royalty, and Varanasi, ”Security in wireless sensor networks,” vol.8,2008.
[10] Chris Karlof and David Wangner, ”Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, IEEE,2003.
[11] M. Razzaque and Ahmad Salehi,“Security and Privacy in Vehicular Ad- Hoc Networks: Survey and the Road Ahead”, Wireless Networks and Security, Springer: 107- 132, 2013.
[12] R. E. Shannon, “Introduction to the art and science of simulation,” in Proc. of the 30th conference on winter simulation (WSC’98), 1989.
[13] Virendra Pal Singh, Aishwarya S. AnandUkey, and Sweta Jain "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks" nternational Journal of Computer Applications (0975 – 8887), Volume 62– No.15, January 2013.
[14] Damandeep Kaur and Parminder Singh "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole attack", IEEE Int. J. on Network Security, Vol. 5, No. 1, January 2014.
[15] NisargGandhewar and Rahila Patel, "Performance evaluation of AODV protocol in Magnetusing NS2 simulator”, 2011.

AUTHORS

Mohammad Abdus Salam is a professor in the Department of Computer Science at Southern University, Baton Rouge, Louisiana, USA. He received his PhD degree from Fukui University, Japan.He is a senior member of IEEE. His research interests include wireless communication, error controlcoding, and sensor networks.

Nayana Halemani earned Masters of Computer Science in 2015 from Southern University, Baton Rouge, Louisiana. She completed her Bachelor's Degree in Computer Science at Visvesvaraya Technological University in, Karnataka, India in 2009. She worked for 2 years as a teaching assistance in engineering college, India. While she was in teaching profession, she took responsibility to teach C programming and data structure C++.