International
Journal
Of Advanced Research in Engineering & Management (IJAREM)
ISSN: 2456-2033 || PP. 34-44

TO PROPOSE A FRAMEWORK – IDPS FOR A MANET UNDER FLOODING ATTACK

Dr. A. Francis Saviour Devaraj*, Mr. Akalu Assefa**
**(Department of Information Technology, School of Informatics, Wolaita Sodo University, Ethiopia)*
*** (Department of Information Technology, School of Informatics, Wolaita Sodo University, Ethiopia)*

Abstract: Mobile Ad-Hoc Network (MANET) is a type of ad-hoc network in which a collection of mobile devices form a network without any infrastructure. MANET is widely used at locations where the fixed infrastructure for communication has been destroyed or in demanding situations such as earthquake, flood, fire explosions, plane/air crash etc. The mobile ad hoc networks depend on the participating node's battery to perform its operation. It is a well known fact that insufficient battery power leads to link failure in the network and it requires re-establishment of the network. Since there is no centralized administration in MANET, it is vulnerable to security threats. Flooding attack is one of the internal/external active security threats. The compromised node sends a large amount of RREQ packets to the neighbor node or massive amount of useless data packets to nodes in the network. Therefore there is a need to propose a frame work - IDPS for a MANET under flooding attack. The proposed framework detects the flooding attack thereby saving bandwidth & battery, by not responding to the bogus request, with the aid of routing table information. The proposed framework also prevents the flooding attack, thereby saving bandwidth & battery, with the aid of information about the battery capacity.

Keywords: DSDV**,** Flooding attack, IDPS, MANET, RWM

1. INTRODUCTION

Ad-hoc network is type of an infrastructure less wireless network and has now become one of the interesting and active areas of research in the field of communication and networking [1].

It is a decentralized, self-organizing, and infrastructure-less network. It is self configurable network [5]. There are many attractive & useful applications of mobile ad-hoc networks (MANETs). There are still some critical challenges and open problems to be solved [1]. Flooding attack is a deadly attack in MANET that consumes battery power of node and bandwidth of the network.

This paper aims to propose a framework for an intrusion detection and prevention system for a MANET under flooding attack. The rest of the paper is organized as follows: Section two discusses about the related work. The materials and methods of the study is discussed in section three. Section four elaborates about the results and the discussions of the results. Section five presents the conclusions.

2. RELATED WORK

In this section, the related work of the proposed intrusion detection and prevention system is literature reviewed.

2.1. Intrusion Detection and Prevention System (IDPS) [3, 11]

In today's world, the whole system is going digital, that means all the information are being stored in digital machine instead of traditional way. Thus when digital communities that are depending on computer technology want to share valuable/secret information to a person in any corner of the world or nearby, it is mandatory to keep the network safe from intruders/hackers/attackers. In order to safeguard the information from these intruders, there emerged a technique called Intrusion Detection and Prevention System (IDPS).

2.2. Existing Intrusion Detection and Prevention System for MANET with Flooding Attacks

2.2.1. Preventing flooding attack in MANETs using the reserved bits of AODV messages [16]

The problem of flooding attack is tackled, and a solution is proposed to prevent flooding attack as follows: The technique used to prevent the flooding attack in this approach is the use of reserved bit RREQ message. It is concluded that using the reserved bits, both route request and data flooding attacks can be

completely prevented from external attackers and the attackers are isolated from the network by their respective neighbors.

2.2.2. A new flooding attack prevention (FAP) in mobile ad-hoc networks [12]

It proposed a new Flooding Attack Prevention (FAP) mechanism – neighbor suppression and path cutoff. The main idea of neighbor suppression is that each neighbor calculates the rate of RREQ originated by an intruder. This method eliminates the flooding packet but if the intruder has the idea about the threshold value then it can bypass the threshold prevention (TP) mechanism. The study found that the prevention is more effective for higher flooding rates.

2.2.3. Performance analysis of flooding attack prevention algorithm in MANETs [14]

This prevention scheme is concluded that upto maximum trusted level, the RREQ and data packet reached to destination normally and the RREQ and data packets beyond maximum trust level dropped or ignored.

2.2.4. Follow ship: defense against flooding and packet drop attacks in MANET [17]

The architecture of the scheme comprises three operational components namely rate-limitation component, enforcement component and restoration component. Rate-limitation minimizes the flooding attacks while the enforcement component reduces the packet drop attacks. And the restoration component is used to resolve the ambiguity between the intentional and accidental drops. If the packets generated by the neighbor exceed the transmission-threshold within the given interval, then the neighbor is expected to be malicious or selfish and the packet is discarded. But, the proposed solution is not verified mathematically or using simulation. Although the solution is proposed to prevent flooding and dropping attacks, it uses rate limitation to prevent flooding attack which is ineffective at lower attack rates and if the attacker possesses knowledge about the rate limit.

2.2.5. Examination of impact of flooding attack on MANET and to accentuate on performance degradation [9]

In this flooding attack prevention system, the attackers usually use any one of these following scenario for generating the attack traffic. In scenario1, the attacker will send excess amount of route request packets to the destination without adhering to the rate limit parameter. In scenario2, the attackers will attack from different origin with fewer amounts of RREQ packets by adhering to rate limit. This case is highly difficult to detect as the attack is originating from different nodes. Further it is also difficult to identify this type of attack packets from that of normal one which is send by genuine node because of link break or stale route. They proposed detection scheme for attackers.

The proposed detection scheme which aims at detecting the malicious node which sends the bogus RREQ packets.

3. MATERIALS AND METHODS

Research methodology defines how the work should be carried out in a research community [13]. In this section, the research framework, the approaches of study, techniques and variables or parameters are discussed in detail.

3.1. Research Methodologies

The researcher divides the whole thesis work into four phases.

Phase1: **LITERATURE REVIEW**

In this phase the researcher had reviewed a lot of literature and understood about MANET, applications of MANET, routing protocols of MANET (DSDV), mobility models of MANET and security attacks in MANET and existing IDPS of flooding attack.

Phase2: **PROBLEM IDENTIFICATION AND DESCRIPTION**

This phase is the most important phase, where the problem was identified and described. (i.e.) the performance of MANET with IDPS is affected due to flooding attack

Phase3: **PROPOSE A FRAMEWORK FOR IDPS**

In this phase the researcher proposed a framework for an IDPS in MANET under flooding attack.

Phase4: **RESULT ANALYSIS, DISCUSION and CONCLUSION**

Then the performance of the network under flooding attack with and without IDPS is analyzed. Finally, discussion was made and conclusion was drawn.

3.2. Proposed Technique to Detect and Prevent Attack

The proposed framework for intrusion detection and prevention technique minimizes RREQ flooding attack and saves the resources like bandwidth and battery of a legitimate node. In proactive routing protocol each node maintains a routing table and broadcasts it to the neighbor nodes even if there is no change in network topology. Then the neighbor nodes waste resources like battery, bandwidth by sending reply message (RREP) or error message (RRER). An attacker node uses this to its advantage and sends massive amount of useless and non updated RREQ packets to their neighbors to receive RREP or RRER message. In order to solve such kind of problem, we propose a framework for an intrusion detection and prevention system.

To propose a framework for an intrusion detection and prevention system, we have considered two scenarios.

Scenario1; detects the intrusion

The detection technique uses routing table information of DSDV routing protocol. Routing table contains, all available destinations, the next hop, distance /metric and destination sequence number.

The attacker node floods as follows; First, attacker sends RREQ (updated or not updated) and waits for RREP or RRER packets. So neighbor node will be kept busy in receiving RREQ and sending RREP or RRER packets rather than performing normal operation. The proposed framework for IDPS handles this scenario in the following ways:

1. The proposed framework for IDPS checks the routing table of Node A. If the request is not updated one, the IDPS just ignores by not replying-thereby saving the resources (bandwidth and battery).
2. If it is a genuine RREQ, then the proposed framework for IDPS, checks the battery capacity of neighbor node and the attacker node. If both nodes satisfy the minimum required battery capacity to perform communication, then IDPS allows the neighbor node to respond.

Scenario2; prevents the intrusion

The prevention technique uses the information about battery capacity of the sending and receiving nodes. The proposed framework for IDPS proactively prevents an attack by checking the capacity of batteries of the communicating nodes as follows:

1. The battery capacity of the malicious node will always be much lesser than the genuine node.
2. To perform a communication (RREQ and RREP or RRER), it is required by the participating nodes to possess a minimum battery capacity. If the required minimum battery capacity for a communication is not satisfied, the proposed framework for IDPS will prevent the communication(RREQ and RREP) from taking place

3.2.1. Flow chart diagram for intrusion detection and prevention

In this section, we propose the flow diagram for the framework of an IDPS.

Flow chart diagram for detection

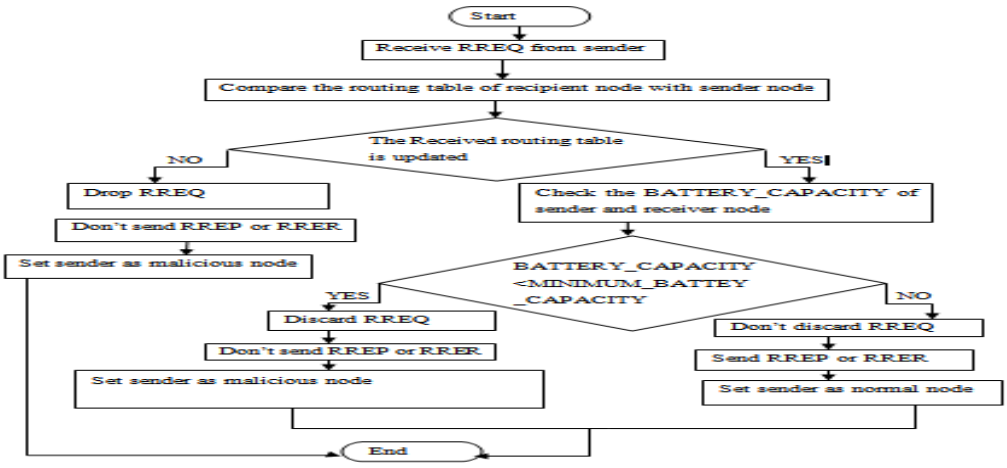

Fig 1: Flow chart diagram for intrusion detection

Flow chart diagram for prevention

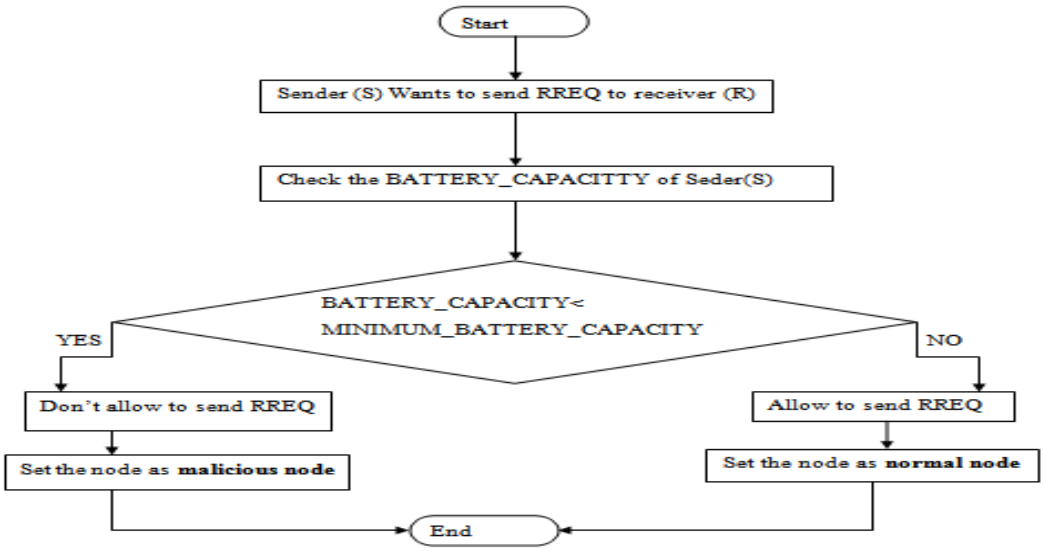

Fig 2: Flow chart diagram for intrusion prevention

4. RESULTS AND DISCUSSION

In this section the logic behind the proposal is furnished as numerical examples and the results are discussed.

4.1. Logic

In MANET, two problems that may occur frequently are: count to infinite problem and routing loop problem. When flooding attack happens, the neighbor nodes responds by sending RREQ/RERR, if it doesn't have awareness. Hence, the battery of the node drains unnecessarily. Eventually the nodes gets shutdown. So the node becomes unreachable. The metric for the dead node is set to infinite.

For example, with reference to the network topology as shown in Figure 3, there are six nodes namely A, B, C, D, E, & F. For instance, A is the source node and D is the destination node. The possible routes are A-B-C-D or A-F-D. Meanwhile, node E becomes an attacker and starts flooding to its neighbor nodes (B, C & F). Without knowing E as an attacker, nodes B, C & F responds and loses its battery backup. Hence, nodes (B, C & F) may get shut down sooner or later. Eventually B, C & F are intermediate nodes in the path from node A to node D, the metric is made to infinite. Then the possibility of the packet from node A reaching to node D is not possible. Count to infinite problem had occurred. Also the packet keeps looping without able to reach the destination-routing loop. As per the study, DSDV eliminates count to infinite problem and routing loop problem [15].

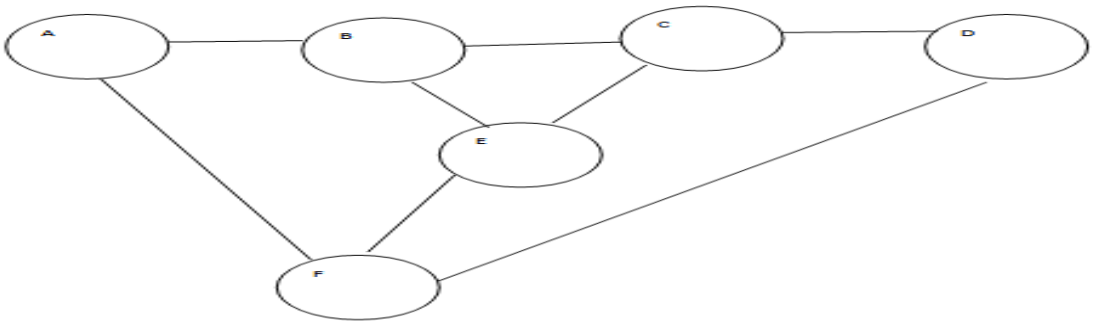

Fig3: Sample network topology

Detection;

For example, with reference to RFC 3561 [7], the following facts are used. The maximum number of RREQ packets per second is 10. The battery capacity of participating nodes in the simulation area is 3.8v. The nodes considered in this thesis confines to IEEE 802.11b.With reference to IEEE 802.11 [8], the maximum capacity of wireless link for 802.11b standard is 11mbps.

Assumptions;

1) The Bandwidth required for 1RREQ and 1 RREP or 1 RRER is 512kbps.
2) The Maximum number of RREQ/s for genuine node is 6.
3) The maximum number of RREQ/s for attacker node is 9.
4) The energy consumed for one communication is 5% of 3.8 V. For RREQ 2.5% of 3.8v of and for RREP or RRER 2.5% of 3.8v
5) The maximum speed of a node is 20m/s.
6) The node movement happens once in 25 sec.
7) The maximum simulation time is 100 sec.
   4 times the node movement happens approximately.
   When the node link breaks?
8) Genuine node speed is 10 m/s.
9) Attacker node speed is 20 m/s
10) From 0 to 24 sec there is no attack.
    After 24 sec attack happens. During that time attacker node moves faster than genuine neighbor node.
    Chance of link break to happen is at 25 sec, 50 sec and 75 sec
11) Attacker node sends 9RREQ/s
12) Energy consumed = 9*2.5% of 3.8v=9*0.095v=0.855v
13) Genuine node 6 RREQ/s
14) Energy consumed 6* 2.5% of 3.8 v= 6*0.095v=0.57v
15) IDPS allows communication only when battery capacity is the minimum of 25% (0.95v)

4.1.1. The energy consumed by nodes without attack and with attack

Starting from 0 to 24sec genuine node as well as malicious node move with equal speed and consume the same energy. Which means the maximum speed of genuine node and malicious node are 10m/s and the maximum battery capacity consumed by genuine and attacker node is 0.57v. The attacker node increases his movement speed to 20 m/s. This increases the probability of link break. Using this opportunity attacker node fires more RREQ. Approximately attack happens three times (25^{th} Sec, 50^{th} Sec, and 75th Sec) which mean attack will happen between 25 & 100 sec. The energy consumption of a node with and without flooding attack is discussed in the following table 1

Table 1: The result of battery capacity consumed by nodes without and with attack

Time interval	Speed of Genuine node	Maximum battery consumed by genuine node	Maximum speed of attacker node	Maximum battery consumed by attacker node
0-24 sec	10m/s	0.38v	10m/s	0.38v
25-49 sec	10m/s	1.33v	20 m/s	1.61v
50-74 sec	10 m/s	2.28v	20 m/s	2.84v
75-99 sec	10 m/s	3.23v	20 m/s	4.07v

4.1.2. The battery capacity consumed by nodes without attack and with attack plus IDPS

In table 1 all the nodes are moved with equal speed and consumes equal battery power from 0 second to 24 seconds. Between time interval 0 and 24 seconds every nodes are acting as genuine node. Starting from 25 seconds to 49 seconds for the first time the attacker node generated the large amount of useless RREQ packets to genuine nodes thereby consumes more battery power and moves faster than genuine node. Starting from 50 seconds to 74 seconds for the second time the attacker node generated large amount of useless RREQ packets to genuine nodes thereby consumed more battery power and moved faster than genuine node. Starting from 75 seconds to 99 seconds for the third time the attacker node generated the large amount of useless RREQ packets to genuine nodes thereby consumed more battery power and moved faster than genuine node.

The framework proposed for IDPS starts functioning at 25 seconds. After 25seconds the IDPS compares the routing table received with the recipient node's routing table, if the received routing table is updated, the IDPS treats the sender as genuine node. If the received routing table is not updated the recipient node treats the sender as a malicious node. Minimum of 20 % of battery power must be required for one communication. If the remaining amount of battery is less than 20 % , the node also discards RREQ even if the received routing table is updated. In the following section, we are going to discuss how IDPS saves resources by detecting and preventing flooding attack.

A) Network topology at time 0 sec

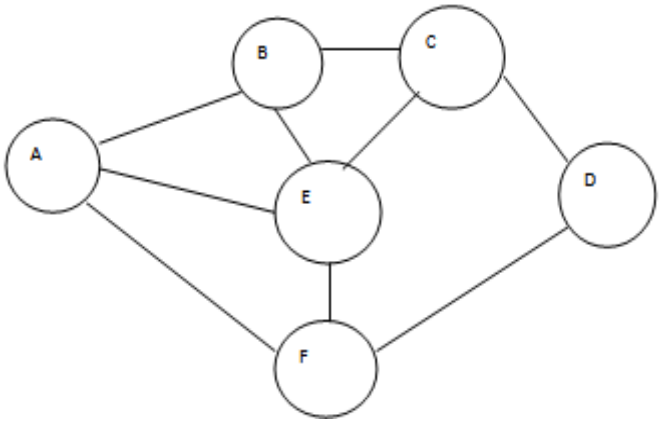

Fig 4: Network topology at time 0 sec

Table 2: Results of resource consumed and saved by nodes without attack & with attack plus IDPS

s. no	Time Interval	Node speed		Battery consumption		IDPS action		Resource saved	
		genuine	Attacker	Genuine	Attacker	Detection	Prevention	battery	bandwidth
1	0-24s	10m/s	10m/s	10% (0.38v)	10% (0.38v)	-	-	-	-
2	25-49s	10m/s	20m/s	1.33v	1.61v	✓	-	0.57v	512kbps
3	50-74s	10m/s	20m/s	2.28v	2.84v	✓	-	0.57V	512kbps
4	75-99 s	10m/s	20m/s	3.23v	4.07v	✓	✓	0.57v	512kbps

In figure 4, assume E is an attacker node. A is the source node. D is the destination node. So node A communicates with node D via B and F. A, B, C and F are neighbor nodes to E.

In table 2, for the time interval between 0 second and 24 seconds, the node speed of genuine node and attacker node is 10m/s (i.e. there is no attack). The processing work and miscellaneous work consumes 10 % of the battery (0.38v). The IDPS is not active at this time. Hence, there is no saving of resources.

B) Network topology at time 25 sec

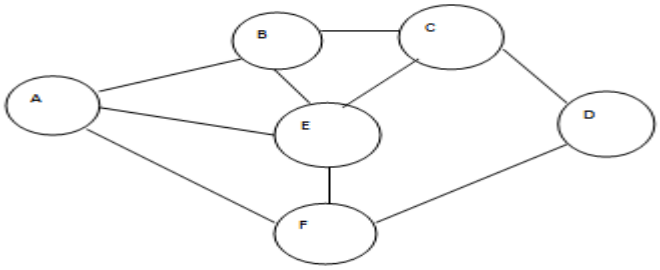

Fig 5: Network topology at time 25 sec

The network topology at time 25 seconds is given in figure 5. When compared to topology at time 0 second (figure 4), there is no change. So, there is no change in the routing tables of the nodes.

In table 2, for the time interval between 25 seconds and 49 seconds, the node speed of genuine node and attacker node is 10m/s and 20m/s respectively. The battery consumption of the genuine node and attacker node is 1.33 v and 1.61v respectively. The calculation of energy is as follows:

i) Genuine node

Up to 24 seconds battery consumed = 0.38v

Between 25 second to 49 second battery consumed = 0.95v (0.57v + 0.38V)

Total battery consumed up to 49 second = 1.33v

ii) Attacker node

Up to 24 seconds battery consumed = 0.38v

Between 25 seconds to 49 seconds battery consumed = 1.23 (0.85v + 0.38V)

Total battery consumed up to 49 seconds = 1.61v

The attacker node E has increased its moving speed. As per our assumption, attack happens after 24 seconds. During this time, the attacker node E sends bogus RREQ to its neighbor nodes. The IDPS in the neighbor nodes verifies the routing table and finds that there is no change in topology. So the IDPS action is detection of flooding attack. Since the IDPS has detected the flooding attack, it doesn't respond to RREQ. Thereby neighbor nodes saving the battery by 0.57v and bandwidth by 512kbps.

C. Network topology at time 50 sec

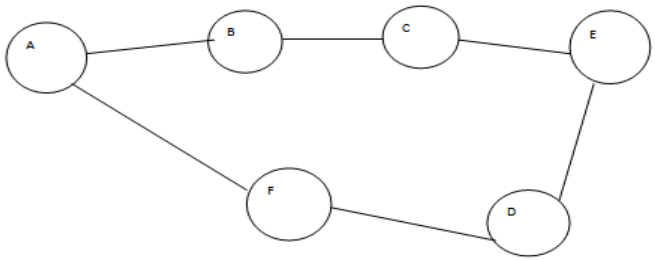

Fig 6: Network topology at time 50 sec

The network topology at 50 seconds is as shown in figure 6. The neighbor nodes of the attacker Node E are node C and D.

In table 2, for the time interval between 50 seconds and 74 seconds, the node speed of genuine node and attacker node is 10m/s and 20m/s respectively. The battery consumption of the genuine node and attacker node is 2.28 v and 2.84v respectively. The calculation of energy is as follows:

i) Genuine node

Up to 49 seconds battery consumed = 1.33v
Between 50 seconds and 74 seconds battery consumed = 0.95v (0.57v + 0.38V)
Total battery consumed up to 74 seconds = 2.28v

ii) Attacker node

Up to 49 seconds battery consumed = 1.61v
Between 50 seconds and 74 seconds battery consumed = 1.23 (0.85v + 0.38V)
Total battery consumed up to 74 seconds = 2.84v

The attacker node E has increased its moving speed. As per our assumption attack happens once in 25 seconds. During this time, the attacker node E sends bogus RREQ to its neighbor nodes (C and D). The IDPS in the neighbor node C verifies its routing table and finds that there is no change in routing table. So the IDPS action is detection of flooding attack in node C. Since the IDPS has detected the flooding attack, it doesn't respond to RREQ. Thereby, saving the battery by 0.57v and bandwidth by 512kbps.

D) Network topology at time 75 sec

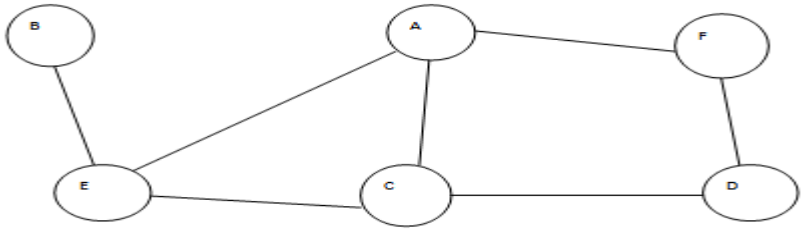

Fig 7: Network topology at time 75 sec

The network topology at 75 seconds is as shown in figure 7. The neighbor nodes of the attacker Node E are nodes A, B and C.

In table 2, for the time interval between 75 seconds and 99 seconds, the node speed of genuine node and attacker node is 10m/s and 20m/s respectively. The battery consumption of the genuine node and attacker node is 3.23 v and 4.07v respectively. The calculation of energy is as follows:

i) Genuine node

Up to 74 seconds battery consumed = 2.28v
Between 75 seconds and 99 seconds battery consumed = 0.95v (0.57v + 0.38V)
Total battery consumed up to 99 seconds = 3.23v

ii) Attacker node

Up to 74 seconds battery consumed = 2.84v
Between 75 seconds and 99 seconds battery consumed = 1.23 (0.85v + 0.38V)
Total battery consumed up to 74 seconds = 4.07v

The attacker node E has increased its moving speed. As per our assumption attack happens once in 25 seconds. During this time, the attacker node E sends bogus RREQ to its neighbor nodes (A, B and C). The IDPS in the neighbor nodes of A, B and C verify its routing table and finds that there is a change in their routing tables. But, the IDPS of nodes A, B and C prevents the flooding attack, since the battery of node E is dead. Since the IDPS has prevented the flooding attack, it saved the bandwidth by 512kbps as well as the battery of nodes A, B and C by not responding.

4.1.3. Battery and bandwidth consumption and saving by nodes at given interval of time

With reference to table 1 & 2 the battery and bandwidth consumption and saving by each node is discussed as follows:

In table 3, between time interval 0 second and 24 seconds, the topology used is as shown in figure 4. In table 3 between time interval 0 and 24 seconds 10% (0.38v) of battery is consumed by each node of figure 4. As per our assumption, there is no attack at this interval of time. At this time interval, the RREQ is not generated and sent by any node and so the RREP or RRER message is not replied from any node. The 10% (0.38v) of battery is consumed for processing power and miscellaneous work only. Also at this time interval bandwidth is not consumed by any node because RREQ packets are not generated and so RREP or RRER packets are not sent by any node.

In table 3, between time interval 25 seconds and 49 seconds, the topology used is as shown in figure 5.Until this time interval, the total amount of battery consumed by attacker node E and neighbor nodes (A, B, C &F) are 1.61v and 1.33v respectively. When we compare network topology of figure 4 at time interval 0 and 24 second and figure 5 at time interval 25 seconds and 49 seconds, there is no change in the network topology. Both of the topologies are similar. Node E starts flooding attack, by sending bogus RREQ. But IDPS is active at time interval 25 seconds and 49 seconds and performs the detection action. When an IDPS at each neighbor nodes perform detection, it detects that he received RREQ packet by neighbor nodes are not updated one. So that, received RREQ packets by each neighbor nodes are discarded and RREP or RRER packets are not sent to node E. Therefore, 0.57v of battery consumption for sending RREP or RRER packets by all neighbor nodes (A, B, C and 0.512kbps of bandwidth of link between E and all neighbor nodes required for sending RREP or RRER packets are saved.

In table 3, between time interval 50 seconds and 74 seconds, the topology used is as shown in figure 6. Until this time interval, the total amount of battery consumed by attacker node E to send RREQ packets and neighbor nodes (C & D) to receive RREQ packets are 2.84v and 2.28v respectively. When we compare routing table of node E for figure 6 and routing table of node E for figure 7 there is change for route from node E to node D and there is no change for node E to node C. This means that, node E sent updated RREQ packets to neighbor node D and not updated RREQ packets to neighbor node C. IDPS is active at time interval between 50 and 74 seconds and performs the detection action. IDPS at each neighbor nodes(C & D) perform detection and learns that, the received RREQ packet for neighbor node D is updated one and for neighbor node C is not updated one. So that, the RREP or RRER packets from neighbor node D are sent to node E. But RREQ packets received by neighbor node C are discarded and also RREP or RRER packets are not sent to node E. So that, 0.57v of battery consumption for sending RREP or RRER packets by neighbor node C and 0.512kbps of bandwidth required between link of neighbor node C and node E is saved.

In table 3, between time interval 75 and 99 seconds, the topology used is as shown in figure 7. Until this time interval, the total amount of battery consumed by attacker node E and neighbor nodes (A, B & C) are 4.07v and 3.23v respectively. When we compare routing table of node E for figure 6 and routing table of node E for figure 7 there is a change in route from node E to A & B. But there is no change in route from node E to node C. This means that node E sent updated RREQ packets to neighbor node A and B, but not to neighbor node C. IDPS is active between time interval 75 seconds and 99 seconds and performs the detection as well as prevention action. Because of battery capacity of neighbor nodes (A, B & C) is less than minimum battery capacity IDPS also performs prevention at this time interval. When an IDPS at each neighbor node performs detection action, it

detects that the received RREQ packets by neighbor node A and B are updated one and the received RREQ packets by neighbor node C are not updated one. When IDPS performs prevention action, it finds that the battery capacity of neighbor nodes (A, B&C) is less than minimum battery capacity required for communication. So that, received RREQ packets by neighbor node A, B and C discarded & RREP or RRER is not sent to node E. Therefore, 0.57v of battery consumption for sending RREP or RRER packets by neighbor nodes and 0.512kbps of bandwidth required between link of neighbor nodes and node E is saved.

Total amount of battery consumed and remained (available) by each node is summarized in table 3 as follows.

Table 3: Total amount of battery consumed and remained (available) by each node at given time interval

Time interval	Node A		Node B		Node C		Node D		Node E		Node F	
	C	R	C	R	C	R	C	R	C	R	C	R
0-24s	0.38v	3.42v	0.38v	3.42v	0.38v	3.42v	0.38v	3.42v	0.38v	3.42v	0.38v	3.42v
25-49s	1.33v	2.47v	1.33v	2.47v	1.33v	2.47v	0.76v	3.04v	1.61v	2.19v	1.33v	2.47v
50-74s	1.71v	2.09v	1.71v	2.09v	2.28v	1.52v	2.28v	1.52v	2.84v	0.96v	1.71v	2.09v
75-99s	3.23v	0.57v	3.23v	0.57v	3.23v	0.57v	2.66v	1.14v	4.07v	-0.27v	2.09v	1.71v

Where C is consumed battery, R is remained battery.

According to table 4 below, we prove that the proposed framework for IDPS for a MANET under flooding attack saves considerable amount of battery and bandwidth. The battery and bandwidth saved by each node are summarized in table 4 as follows.

Table 4: The battery and bandwidth saved by each node at given time interval

Time interval	Node A		Node B		Node C		Node D		Node E		Node F	
	B	B	B	b	B	B	B	b	B	b	B	b
0-24s	-	-	-	-	-	-	-	-	-	-	-	-
25-49s	0.57v	512kb/s	0.57v	512kb/s	0.57v	512kb/s	-	-	-	-	0.57v	512kb/s
50-74s	-	-	-	-	0.57v	512kb/s	-	-	-	-	-	-
75-99s	0.57v	512kb/s	0.57v	512kb/s	0.57v	512kb/s	-	-	-	-	-	-

Where B is battery saved and b is bandwidth saved

5. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1. Summary

MANET has become an effective & easy means to network devices in demanding situations. The vulnerability nature of the MANET posses huge security challenges. One of the challenging attack is a form of denial of service (DoS) attack called “flooding attack”. The constrains of the nodes in MANET are battery capacity of the node and bandwidth of the network. Therefore it is essential to optimally use the battery of the node and bandwidth of the network. This requirement motivated us to take up this research work. The random way mobility model contributes to the optimal usage of bandwidth of the network and battery of the node when compared to other mobility models. A lot of previous research work had been done on the study of the performance of a MANET with and without flooding attack. The researchers have proved that, the performance of the MANET had degraded in terms of throughput, end-to-end delay and packet delivery ratio. A framework for an IDPS for a MANET with flooding attack was proposed and discussed.

5.2. Conclusions

With reference to the results and discussion we had from chapter four the following conclusions have been made:

i) It is learnt that the MANET can be setup in adhoc mode, thus saving lot of time and money.

ii) As per table 2, the proposed framework may perform detection and prevention as on when required.

iii) As per table 2, the proposed framework may save battery a minimum of 0.57v and a minimum of 512kb of bandwidth per second.

iv) The proposed framework for IDPS smartly uses RREQ received from attacker, to update the routing tables of the neighbor nodes, but saves the bandwidth of the network and battery of the genuine node by not responding.

v) The data flooding attack has not been considered.

vi) The proposed frame for IDPS will necessarily add overhead, however, the end results may save considerable battery of the node and bandwidth of the network.

vii) The proposed framework for the IDPS is not scalable.

5.3. Recommendations

The following of the research problems thrown for future researchers:

i) In this thesis work we only concentrated with RREQ flooding attack and used routing table of nodes to detect attack and minimum battery capacity to prevent attack. There is also DATA flooding attack which degrades the performance of MANET by consuming bandwidth of the network and battery of the network.

ii) In future a light weight IDPS may be developed, so as to decrease the overhead created by IDPS.

iii) A more scalable routing protocol might be used.

6. REFERENCES

[1]. Ankur O. Bangand Prabhakar L. Ramteke. 2013. MANET: History,Challenges And Applications. International Journal of Application or Innovation in Engineering & Management Vol.2 Issue 9.

[2]. Apurva Sharma, Dr. Gurpreet and Er.Jaswinder Singh. 2013. MOBILITY MODELS FOR MANET: MATHEMATICAL PERSPECTIVE. International Journal of Advanced Research in Engineering and Applied Sciences ISSN: 2278-6252 Vol. 2 No. 5.

[3]. Bilal Maqbool Beigh , Uzair Bashir and Manzoor Chachoo . 2013. Intrusion Detection and Prevention System: Issues and Challenges.International Journal of Computer Applications (0975 – 8887) Volume 76 No.17.

[4]. D. Charles Engelhart, Christopher L. Barrett, Monique Morin**.** A Spatial Analysis of Mobility Models: Application to Wireless Ad Hoc Network Simulation.

[5]. https://en.wikipedia.org/wiki/Ad_hoc: [accessed March 2017).

[6]. https://en.wikipedia.org/wiki/Random_waypoint_model [accessed, March 18/2017].

[7]. https://tools.ietf.org/html/rfc3561 [accessed at April 19/2017].

[8]. http://wirelessdmx.com/wp-content/uploads/2016/07/Review-of-the-802.11-standards-2-spalter.pdf [accessed,March 18/2017]

[9]. K. Bhuvaneshwari and A. Francis Saviour Devaraj. 2013. Examination of impact of flooding attack on MANET and to accentuate on Performance degradation. Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 ISS: 0975-0290: Pages: 1695-1699

[10]. Mohit Kumar and Rashmi Mishra . 2012. An Overview of MANET: History, Challenges and Applications. Indian Journal of Computer Science and Engineering ISSN: 0976-5166 Vol. 3 No. 1 pp.121-125.

[11]. Peter Stavroulakis and Mark Stamp. Intrusion Detection and Prevention Systems. Handbook of Information and Communication Security.

[12]. Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong. A New Routing Attack in Mobile Ad Hoc NetworksVol. 11 No. 2.

[13]. Radhika Saini , Manju Khari. 2011. Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network. International Journal of Computer Applications Volume 20– No.4.

[14]. Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao. 2009. Performance Analysis of Flooding Attack Prevention Algorithm in MANETs. World Academy of Science, Engineering and Technology.

[15]. Tao Wan, Evangelos Kranakis and Paul C. van Oorschot. 2004 Securing the Destination-Sequenced Distance Vector Routing Protocol (S-DSDV). *Springer-verlag berlin Heidelberg*, 3269.

[16]. Teklay Gebremichael. 2014 Preventing Flooding Attack in MANETs using the reserved bits of AODV messages. Addis Ababa institute of technology school of electrical and computer engineering.

[17]. V.Balakrishnan ,V.Varadharajan and U. Kiran Tupakula . 2006. Followship: Defense against Flooding and Packet Drop Attacks in MANET. Proceedings of IEEE Security & Privacy in Emerging Areas.