ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.7

An Efficient Detection Mechanism of Opposing the Packet Faking Attack in Opportunistic Networks

Dr.T.Pandikumar[1], Atnafu Abrham[2]
Associate Professor[1], M.Tech Student[2]
Department of Computer & IT
College of Engineering, Defense University, Debre Zeyit, Ethiopia

Abstract:
Opportunistic networks (OppNets) are an interesting topic that is seen to have a promising future. Security is a major challenge in Opportunistic Networks (OppNets) due to its characteristics of being an open medium with dynamic topology, frequent partitions, long delays, neither centralized management nor clear lines of defense. Embedding security into these protocols is challenging and has taken a lot of attention in research. A packet dropping attack is one of the major security threats in OppNets as neither source nodes nor destination nodes has any knowledge of when or where a packet will be dropped. To increase the security levels in OppNets, the efficient detection Algorithm is a significant mechanism or solution as observed from published paper. In this research, an efficient attack (packet faking attack) and detection mechanism against a special type of packet dropping where the malicious node drops one packet or more and injects a new fake packet instead is planned to discuss. The Algorithm and mathematical models as observed from the research paper is efficient to detect against this type of attack where each node can detect the attack instead of the destination node. The main clue of the research as it is observed from published papers discusses a very simple yet powerful idea that is the packet creation time of each packet, detection rate, and good network traffic reduction (network congestion reduction). The mechanism is not capable of being applied to trace back malicious node. And nothing more, based on the outcomes from the detection of the attack, the legitimate node can trace back and find the malicious node (Research gap).

Keywords: Denial of service, malicious node detection, Opportunistic network, Packet-dropping-attacks, Security

1. INTRODUCTION

The opportunistic network (OppNets) is an extension of Mobile Ad hoc Network (MANET). Wireless networks‟ properties, such as disconnection of nodes, network partitions, mobility of users and links‟ instability, are seen as exceptions in traditional network. This makes the design of MANET significantly more difficult. Opportunistic networks [2] are created out of mobile devices carried by people, without relying on any preexisting network topology. Opportunistic networks consider disconnections, mobility, partitions, etc. as norms instead of the exceptions. In opportunistic network mobility is used as a technique to provide communication between disconnected “groups” of nodes, rather than a drawback to be solved [7]. It refers to a number of wireless nodes that opportunistically communicate with each other in the form of “Store—Carry—forward” when they come into contact with each other without proper network infrastructure [1][2][4]. Due to these characteristics, OppNets have gained significant research attention due to the security and privacy challenges that have emerged [1][3][4]. A packet dropping attack is one of the major security threats in OppNets. **Packet dropping attacks happen when a malicious node intentionally attempts to drop some of the packets it receives. When a source node sends a message to the destination, any intermediate node could be a malicious node that performs the packet dropping attack.** It can be classified as a denial of service attack (DoS) where the malicious node drops all or some of the packets. This attack is one of the most difficult attacks since neither the source node nor the destination node has the knowledge of where or when the packet will be dropped [1-5]. Packet dropping can degrade the performance of the network and may obstruct the propagation of sensitive data [1-5]. It is a significant challenge to deal with such an attack since the unreliable wireless communication and resource limitations can result in communication failure and result in the wrong prediction about the presence of a packet dropping attack [1-5]. Moreover, a node’s resource, such as energy and bandwidth can be the real reasons behind packet dropping. A power shortage or communication failure, such as physical damage can make a node unavailable. Therefore, it is difficult to recognize whether packets were dropped due to a security attack or for non-security reasons [1-5]. Dropping packets can lead to an increase in the number of packet retransmissions, transfer time, response time and network overhead. However, there is no doubt about the malicious behavior if the node drops some legitimate packets and then injects fake packets to replace them. In this case, the malicious node obviously has enough resources to do this [1]. In packet, faking attack malicious node can selectively drop some packets and inject fake packets so it can maintain the original total number of packets originated from the sender node [1][2]. As it is observed from published paper, packet dropping attacks is not unique to OppNets. Many researchers have been studied before in the context of ad hoc networks and wireless sensor networks [3][4]. However, the existing packet dropping defense mechanisms, such as the multipath routing based mechanisms, reputation based mechanism, data provenance based mechanisms, acknowledgement based mechanisms, are inefficient in OppNets as we do not have end to end connections and usually have no alternative paths from the sender to the destination or vice versa. Network coding based mechanisms are also inefficient as the destination nodes are

required to have a copy of all neighbor's packets/messages in order to decode its message which is difficult to achieve in OppNets. Encryption techniques are inefficient as well, as we required the use of a secret key which is difficult to manage in OppNets since we have no centralized management. To avoid detection by other mechanisms such as Watchdog and pathrater mechanism an attacker can drop one or more packets and inject fake packets to defeat mechanisms that rely on packet count [1-4]. The algorithm, discussed from the published research papers is very accurate for detecting this type of attack as it relays on the packet creation time of each packet [1].

1.1 Statement of the problem

Due to the characteristics of OppNets, no fixed infrastructure is present and the message is forward through many intermediate nodes, the malicious node selectively drops all or some of the packets and injects fake packets instead. And it can maintain the original total number of packets originated from the sender node. Some of the significant challenge and problem in packet faking attack scenarios are: -

i) Packet faking attack: The malicious node can selectively drop all or some of packets instead. Neither the source node nor the destination node has knowledge of where or when the packet will be dropped.

ii) The unreliable wireless communication and resource limitations can result in communication failure. Due to this, the unreliable prediction about the presence of a packet dropping attack.

iii) Malicious node can easily trigger attacks and the rate of malicious drop is high.

iv) Forwarding opportunities of messages are usually limited, with possibly of higher error rates, and longer delay.

1.2 Scope of the Study

The main objective of the research as it is observed from published papers is to introduce an efficient detection algorithm against packet faking attack in OppNets. The specific objectives are:

i) To define packet faking attacks where the malicious node drops packets and then inject fake packets instead.

ii) To discuss an efficient detection mechanism against packet faking attack in OppNets, where the destination node can accurately distinguish between the legitimate and fake (injected) packets.

iii) To provide an efficient malicious node identification algorithm to identify and quarantine identified malicious node(s).

1.3 Signifance of the Research

The significance of the research from the published paper is defined as: -

i) Each node can detect the attack instead of the destination node.

ii) Good network traffic reduction or **network congestion reduction**.

iii) Achievements of a very high effective and accurate detection rate.

iv) Nicely reduces the malicious node dropping rate.

v) Increased percentages of Accuracy to detect fake packets.

vi) Increased percentages of false negative rate.

1I. LITEARTURE SURVEY

A. **2.1 Each Legitimate Node based Packet Creation Time (PCT) mechanism, 2016 [1]:** PCT detection mechanism is node by node based where each legitimate node can run the algorithm to detect fake packets directly. Propagation of fake packets through the network is prevented as any legitimate nodes can detect and drop fake packets. This mechanism is relying on" Packets Creation Time" of each packet. When a message reaches a legitimate node, the node can compare the packet creation time of each received packet. The node can then detect the fake packet based on a different creation time, as all packets in the same message should have the same creation time or be very close (with a difference of Δt).

From the published research paper, the algorithm is defined by the following assumption: -

i) The sender node should automatically include the packets' creation time within each packet sent.

ii) A malicious node has the ability of dropping legitimate packets and then inject fake packets instead of them but has no ability to modify the packets contents including the packets creation time.

Based on these two assumptions, a legitimate node will learn all of the nodes along packets' path, including the packets creation time.

B. **2.2 Destination node based Packet Creation Time (PCT) mechanism, 2014 [2]**

As observed from the IEEE published paper, the researchers called this detection mechanism as the novel packet faking attack detection mechanism. When the message reaches the destination, the destination node can identify the fake packets. Fake packets should have a creation time that is later than other packets, as all packets on the same message should have the same creation time or very close to it (with a difference of Δt).

C. **2.3 Malicious Node Detection in OppNets Using Hash Chain Technique, 2015 [3]**

Each legitimate node can detect the attack by relying on the hash chain techniques and then trace back the malicious nodes. No more fake packets propagation through the network as the legitimate nodes can stop fake packets propagation and directly classify malicious nodes as malicious.

There are two parts in technique as observed from the published research paper:

i) Detect the attack: When the packets reach any legitimate node, the node can recalculate the hash chain and compares it with the existing chain values that are already injected by the sender in each packet.

ii) Trace back malicious nodes: Based on the first stage outcome, the legitimate nodes can trace back and find the malicious node.

From the published research paper, the algorithm is defined by the following assumption: -

i) Hash chain techniques should be used by the sender node to calculate the chain values for the packets and then automatically include them with each packet.

ii) Malicious nodes can drop some legitimate packets and then inject new fake packets instead of them with new recalculated hash chain values and also can modify the packets contents.

D. **2.4 Malicious Node Traceback in Opportunistic Networks Using Merkle Trees, 2015 [4]**

Each legitimate node can detect the attack by relying on the Merkle tree hashing techniques and then trace back to the malicious nodes. The propagation of fake packets through the network is prevented as the legitimate nodes can stop fake

packets propagation and directly classify malicious nodes as malicious.
There are two parts in technique as observed from the published research paper:
i) Attack Detection: When the packets reach any legitimate node, the node can reconstruct the Merkle root hash value and compares it with the existing values that are already injected by the sender node in each packet.
ii) Nodes Trace back: Based on the first stage outcome, the legitimate nodes can trace back and find the malicious node.
From the published research paper, the algorithm is defined by the following assumption: -
iii) The sender node should build a Merkle tree to get a Merkle root for the message and then inject that root value in each packet's header.
iv) Malicious nodes have the ability of dropping some legitimate packets and then injecting new fake packets instead of them with the ability of modifying its parameters including packet creation time, nodes contact time and Merkle root value.

2.5 Reputation Based Malicious Node Detection[2.2] in OppNets, 2016 [5]

When the reputation value of the number of packet is falls, or drops below the required threshold, the developed algorithm as defined from the published research paper detects its source node as malicious node and decreases the trust value of source node.
From the published research paper, the algorithm is defined by the following assumption: -
i) Intermediate nodes may be malicious, the source and the destination nodes are assumed to be legitimate.
ii) Since we are considering selective packet dropping attacks, at least one packet reaches the destination.

I1I. PACKET FAKING ATTACK AND DETECTION MECHANISM

In packet-faking attack "the novel attack", malicious nodes may selectively drop packets, modify and then injects modified fake packets is known as packet faking attack. In early mechanism to find the number of dropped packets or the number of new injected fake packets are based on the calculations of the total transmitted or received packets. These mechanisms are inefficient to detect the attack when malicious nodes drop some packets and then inject new fake packets [1][2].

The novel detection mechanism is very powerful and accurate [1]. In short, the technique relies on a very simple yet powerful idea, the "Packet Creation Time" [1][2]. When each legitimate node receives all the packets including Packets Creation Time, Nodes' Contact Time, and the number of hops for each packet, it will accurately start to detect any fake packets by sorting the packet creation time of each received packet and then choosing the smallest value in the list. From this scenario, each legitimate node can identify the fake packets should have a creation time that is later than other packets as all packets on the same message should have the same creation time plus or minus a small tolerance(Δt) [1][2].

3.1 Assumptions

In the algorithm approach, the research paper makes the following two assumptions:
i) The sender node should automatically include the packet creation time on each packet sent [1][2].
Ii) Malicious node has the ability of dropping legitimate packets and then inject fake packets and has no ability to modify the packets contents including the packets creation time [1][2]. From these two assumptions, a legitimate node will learn all of the nodes along packets' path, including the packets creation time. Figure 1 show the packets path where c8 is the source of the message, c9 is the destination of the message and t16, t15, w14 are intermediate nodes [1].

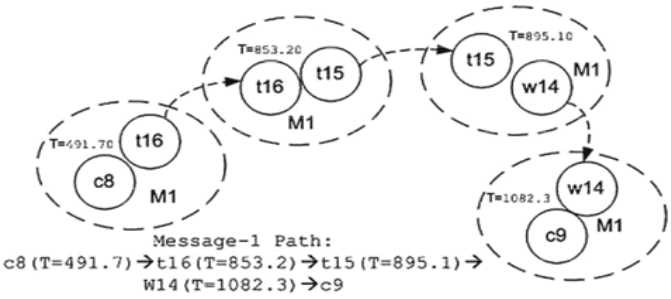

Figure.1. Packets path with packets creation time

3.2 Attack and Defense Scenario

In a fake packet attack, malicious nodes can drop one or more packets (but not all the packets), and instead of them, inject fake packets with the current time of the malicious node. The legitimate node will calculate and find the fake packets. Figure 2 shows the packets' path of message 1(c8—>t16 —>t15 —>w14—>c9), where node t15 drops one packet at time T - 860.2 and then injects a fake packet instead of it [1].

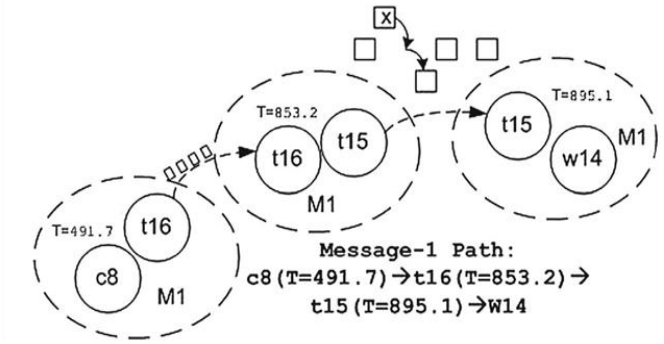

Figure.2. Packet dropping/injecting at malicious node (t15)

There are two phases in Algorithm 1. In phase one, it checked all packets to find and selected the lowest packet creation time. When the legitimate node receives all the packets including Packets' Creation Time (PCT) for each packet, it will accurately start to detect any fake packets by sorting the packet creation time of all received packets and then choosing the smallest value in the list. We will consider that smallest value as a legitimate (PCT) [1][2]. In phase two, it detecting fake packets. The algorithm will continuously check all packets to distinguish and count all fake and true packets. All packets should have the same (PCT) or a very slight difference (Δt). When the malicious node drops packets, it will inject fake packets instead of them at the current malicious node time, therefore the fake (PCT) will always be higher than the original packet creation time of legitimate packets. We may find more than one fake packet creation time (PCT) depending on the number of malicious nodes on the packet's path as we may have more than one malicious nodes sending to each other. If all packets have the same creation time $\pm\Delta t$ then there will be no fake packets and no malicious nodes. As mentioned earlier, in this attack, malicious nodes drop some packets and instead of them, inject fake packets [1][2]. The algorithm is based on the assumption:

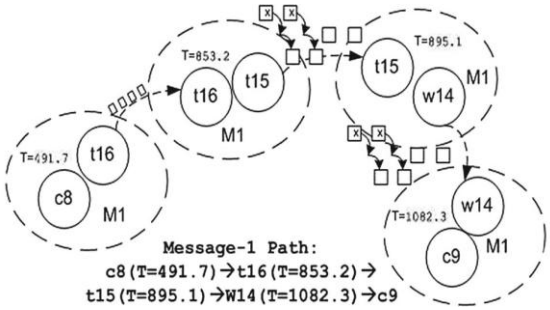

Figure.3. Different sequence packets dropping/injecting on two malicious nodes path

Table.1. Detecting fake packets

Algorithm 1: Detecting fake packets

1: READ: packets Creation Time.
2: Phase 1: Obtain lowest packet creation time
3: For all packets
4: Sort packets Creation Time[i]
5: lowest Packet Creation Time = packets Creation Time [0]
6: packets Are Legitimate = true
7: Phase 2: Detect fake packet(s)
8: For all packets
9: if packets Creation Time[i] = (lowest Packet Creation Time ±Δt) then
10: legitimate Packets Counter++
11: else
12: fake Packets Counter++
13: packets Are Legitimate = false
14: end if
15: if packets Are Legitimate then
16: No fake packets and no malicious nodes, Exit
17: end if

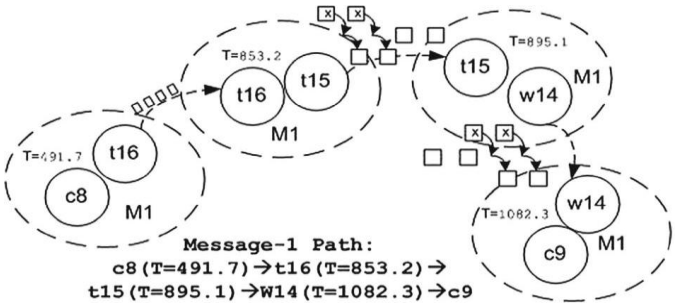

Figure.4. Same sequence packets dropping/injecting on two malicious nodes path

There is at least one legitimate packet at the legitimate node side which has the lowest packet creation time. It can then rely on it and compare it with other packet creation times to find fake packets. However, if "all received packets" are fake or the "same packet sequence" is faked twice or more, then the algorithm will compare it according to the lowest packet creation time to find the fake packets in that message. However, in this case one or more fake packets will be missed and categorized as legitimate. We can see this case in Figure 3 and 4. In Figure 3, there is two malicious nodes on the same path and each one drops/injects different packet sequences. Malicious node (t15) first drops two packets and then sends all four packets to another malicious node (w14). The second malicious node (w14) drops the last two packets and then sends all four packets to the destination (c9) so it will receive four fake packets. In Figure 4, malicious node (t15) drops/injects the first two packets, and then the malicious node (w14) drops/injects two packets in the same sequence (first two packets), and then sends out four packets to the destination (c9). Legitimate node (c9) will not be able to detect the fake packets of malicious node (t15) in either scenario. It can only detect the fake packets of malicious node (w14), and it will recognize the fake packets of (t15) as legitimate packets. However, there is a high probability we can detect the missed fake packets of malicious node (t15) on the other paths, as we will see in the simulation results. The only way to detect all fake packets is to have one or more legitimate packets on the legitimate node side. When we transmit a large number of packets, we will have a better chance of achieving these two conditions, as in the mathematical model.

VI. SIMULATION SETTINGS

As observed from the published paper to test the algorithm, the implemented scenario in ONE simulator [1][2] is using the Epidemic protocol. The simulation was defined to last for 1h, with 0.5s of update intervals [1-5]. Bluetooth was chosen for connectivity with a transmit range of 10M for node radio devices, and transmit speeds of 1000Kbps. There are 12 active nodes composed of cars and pedestrians. Pedestrians and cars have up to 50MB of RAM for storage. Pedestrians move at random speeds between 1 and 1.5 m/s, cars drive only on roads and move at speeds between 10-60 km/h, with wait times of 0-120s. Map Based Movement is used for pedestrians and cars, with a network area of 4500 x 3400M. Nodes move randomly on roads and walkways with a movement warm-up for 10s. There are 3 groups of trams, with 2trams in each group. Map Route Movement is used for trams to follow a constructed tram line. Trams drive at speeds of 7-l0 m/s with a wait time of 10-30s at each configured stop. In addition to the Bluetooth interface, a group of trams uses the high-speed interface with a transmit range of 1000M and a transmit speed of 10Mbps [1-5]. Messages are generated every 1-5 min/node, with message sizes between 50k and look, and a message time to live of 5h. They used the simulator's output as a dataset, and randomly corrupted the dataset based on the number of malicious nodes [1-5]. They then fed the corrupted dataset to the algorithm. Two programs were written using C++. The first program reads the dataset file and then corrupts it by making legitimate nodes malicious by changing the packet creation time for randomly chosen packets and nodes. The second program implements the algorithm, and begins by taking as input the output dataset file generated by program 1 [1][2]. The second program is run to get the algorithm results of the metrics calculations. They also ran the simulator for an average of 30 times to represent each point on the graphs in Figure 5 and 7. [1][2].

4.1 Simulation Results and Analysis

There are used three metrics for evaluating the algorithm,

i) Fake packet detection accuracy: The ratio of the total number of fake packets detected to the total number of actual fake packets [1-5].

ii) False negative rate: The percentage of fake packets have been incorrectly classified as a legitimate packet [1-5].

iii) Network traffic reduction: The ratio of the total number of fake packets detected on the destination nodes side to the total number of the fake packets detected on the node by node side [1].

iv) Malicious path detection accuracy: The ratio of the total number of detected malicious paths to the total number of actual malicious paths [5].

In this scenario, they assumed the source nodes are legitimate

as the source node always will generate the massage and sends packets with the same creation time. And then hand them to the neighbor nodes [1-4]. Neighbor nodes can be malicious or legitimate. However, when the legitimate nodes run the algorithm, it will accurately distinguish between the malicious sender and the legitimate sender. In packet faking attack, the malicious node drops some of the packets, and instead of them injects fake packets with the current malicious node time [1-4]. Dropping and injecting will be on one or more nodes on the same packets' path. In the calculations, researchers assume they have at least one legitimate packet so they can use it as a benchmark comparison [1][2].

In Fig. 4.1, As observed from the published papers researchers can see the packet detection accuracy of the algorithm can achieve 100% accuracy when the percentage of malicious nodes is less than 5 %. This is because there is a good chance for destinations to receive legitimate packets, especially when source nodes transmit large numbers of packets [1][2]. When the number of malicious nodes increases, the accuracy slightly starts to drop as fake packets may be missed when two or more malicious nodes drop and inject packets into the same packet sequence on the same path, as illustrated in Fig. 2.4. However, our algorithm results show the packet detection accuracy does not drop below 78 %, even when 100% of intermediate nodes act as malicious nodes. This is due to the low probability of having two or more malicious nodes dropping and injecting in the same packet sequence on the same path. In addition, the probability of receiving all packets as fake is also low, especially when the sender sends a large number of packets. In our efficient detection mechanism, we always achieved better packet detection accuracy as fake packets will not propagate through the network till it reaches the destination. Any legitimate nodes can stop fake packet propagation, in contrast, our old detection mechanism [1] can detect fake packets only through destination node. Fig 4.2 shows the networks traffic reduction enhance detection mechanism compare to the old detection mechanism [1]. Overall, we have achieved good traffic reduction as each legitimate node can detect fake packets and then stop fake packet from propagation through the network [1][2]. As we can see in Fig. 2.3, we may categorize fake packets as legitimate when we have more than one malicious node sending to each other on the same path where each malicious node fakes a different sequence of packets. This results in having all the received packets at the legitimate node as fake packets. In Fig. 4.3, we can see a zero-false negative rate for our algorithm when we have less than 2 % malicious nodes. This is because of the small number of malicious nodes and the probability of receiving all packets as fake will be very low [1][2].

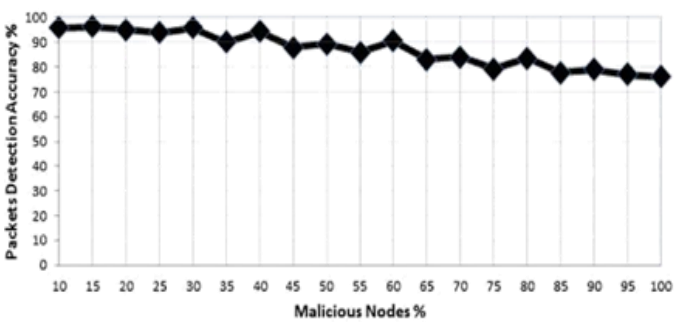

Figure.5. Fake packet detection accuracy as the number of malicious nodes increases

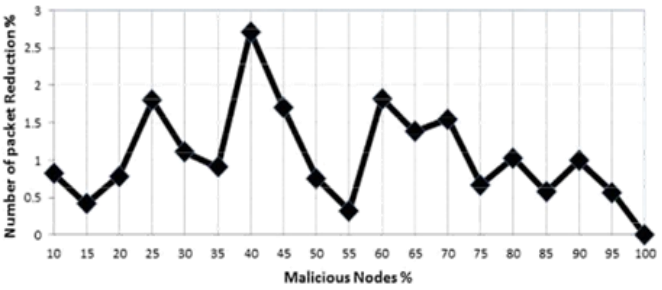

Figure.6. Network traffic reduction

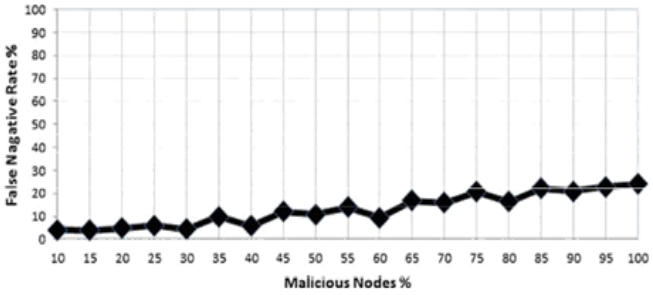

Figure.7. False negative rate as the number of malicious nodes increases

The false negative rate starts to increase slightly till it reaches a maximum of 22 %, and the number of malicious nodes also increase as the probability of receiving all packets as fake also rises.

VI. CONCULSION AND FUTURE WORK

Security is a major challenge in OppNets due to its characteristics, such as open medium, dynamic topology, dependence on cooperative techniques, no centralized management, and absent clear lines of defense. With the absence of an end to end connection, packet dropping attacks have become one of the hardest security threats in OppNets. In addition, neither source nor destination nodes have knowledge of when or where a packet will be dropped in a packet dropping attack. In order to compare this approach with other works focusing on the same subject, the researcher chosen the acknowledgement based mechanisms [5] and the networks coding based mechanism [1-5]. As comparison metrics, they have measured the node detection accuracy. In Figure 4.1, as observed they can see the algorithm achieved a node detection accuracy of 100% when the percentage of malicious nodes are less than 12%. This is because there is a good chance for legitimate node to detect the Packet Creation Time of the malicious nodes as well as the probability of having more than one malicious node sending to each other on the same path will be low as illustrated in Figure 7 [1-5]. In their previous novel attack (Packet faking attack [1][2] they presented a special type of packet dropping where the malicious node drops one or more packets and then injects new fake packets instead. In this paper, as I observe from current research paper, an efficient defense mechanism against this type of attack where each node can detect the attack instead of the destination node. The detection mechanism is very powerful and has very high accuracy. It relies on a very simple yet powerful idea, that is, the packet creation time of each packet. Simulation results show this robust mechanism achieves a very high accuracy, 0 false positive rate, packet dropping rate decreases as the simulation time increases, good detection rate and good network traffic reduction. A lot of work remains to be done as the researcher still do not have a complete solution for a packet dropping attack. Developing new routing protocols with a mechanism for detecting the dropping of all the packets or

some of the packets and modifying these is a real challenge for the future.

VI. REFERENCES

[1].Majeed Alajeely, Asma'a Ahmad, Robin Doss and Vicky Mak-Hau.An efficient detection mechanism against packet faking attack in OppNets. Computational Intelligence and Security (IEEE CIS), 2016 Tenth International Conference on, 15-16 Nov. 2016.

[2].Majeed Alajeely, Asma'a Ahmad, Robin Doss and Vicky Mak-Hau. Packet Faking Attack: A Novel Attack and Detection Mechanism in Opportunistic Networks Opp Nets. Computational Intelligence and Security (CIS),2014 IEEE Tenth International Conference on, Nov. 2014.

[3].Majeed Alajeely, Asma'a Ahmad, Robin Doss and Vicky Mak-Hau.Malicious Node Detection in OppNets Using HashChain Technique. Computational Intelligence and Security (CIS),2015 IEEE12th International Conference on, Nov. 2015.

[4].Majeed Alajeely, Asma'a Ahmad and Robin Doss. Malicious Node Trace back in Opportunistic Networks Using Merkel Trees. Computational Intelligence and Security (CIS), 2015 IEEE12th International Conference on, Nov. 2015.

[5].Majeed Alajeely, Asma'a Ahmad and Robin Doss. Reputation Based Malicious Node Detection inOppNets. 2016 IEEE 13th International Joint Conference on Computer Science and Software Engineering (JCSSE), Nov. 2016.

[6].Majeed Alajeely, Asma'a Ahmad and Robin Doss. Defense against Packet Dropping Attacks in Opportunistic Networks. Computational Intelligence and Security (CIS),2014 IEEE Tenth International Conference on, 2014.

[7].Anshul Verma, Dr. Anurag Srivastava. Integrated Routing Protocol for Opportunistic Networks. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011