Using Trust to Detect Denial of Service Attacks in the Internet of Things Over MANETs

Albandari Alsumayt
School of Science and Technology
Nottingham Trent University
Nottingham, NG11 8NS, UK
albandari.alsumayt2013@my.ntu.ac.uk

John Haggerty
School of Science and Technology
Nottingham Trent University
Nottingham, NG11 8NS, UK
john.haggerty@ntu.ac.uk

Ahmad Lotfi
School of Science and Technology
Nottingham Trent University
Nottingham, NG11 8NS, UK
ahmad.lotfi@ntu.ac.uk

Abstract

The rapid growth of employing devices as tools in daily life and the technological revolution have led to the invention of a novel paradigm; the Internet of Things (IoT). It includes a group of ubiquitous devices that communicate and share data with each other. In order to communicate, these devices use protocols, and in particular, theInternet Protocol (IP) is used to manage network nodes through mobile ad hoc networks (MANET), which provide self-configuring and transient infrastructures. MANET enables each node to freely join or leave the network frequently. IoT is beneficial to MANET as the nodes are self-organising and the information reach can be expanded according to the network range. Due to the nature of MANET, such as dynamic topologies and no administrative point, a number of challenges are inherent, such as message fabrication, confidentiality violations, and Denial of Service (DoS) attacks. DoS attacks prohibit legitimate users from using or accessing their authorised services and is particularly pertinent in IoT systems which rely on persistent connections for the transfer, collection, and processing of data. In addition, because of the high mobility of MANET, the network is likely to merge with other networks. In this situation, two or more networks of untrusted nodes may join one another leaving each of the networks open to attack. This paper proposes a novel method to detect DoS attacks immediately prior to the merger of two MANETs. To demonstrate the applicability of the proposed approach, a Grayhole attack, a type of DoS attack, is used in this study to evaluate the performance of the proposed method in detecting attacks.

Keywords—IoT; MANET; Denial of Service; Trust.

1. Introduction

A mobile *ad hoc* network (MANET) is a group of devices called nodes that communicate with each other without any fixed infrastructure. These devices could be any devices with wireless ability, including an iPhone, iPads, laptops, or MP3 players. MANET is multi-hop and self-configuring. It does not have a central administration point to monitor and control nodes among the network (Jain and Garg, 2013). Every node in a MANET is a router in sending packets and a host in receiving these packets (Jain, 2014). The Internet of Things (IoT) refers to a multitude of peripheral devices that are networked and are managed via the Internet Protocol (IP) (Bellavista et al., 2013). Information about each device or object is gathered using infrared sensors; voice or video sensors; Radio Frequency Identification (RFID), and so on. MANET are ideal in the deployment of IoT infrastructures as the nodes move in an arbitrary and self-organised manner, so the information collection range is expanded (Patil and Pawar, 2016).These benefits have been identified with regards to IoT technologies for the healthcare domain where their application can be grouped into objects or people, such as staff and patients, authentication and identification of people, as well as data collection and sensing (Kulkarni and Sathe, 2014 ; Babu et al., 2016).IoT applications such as tracking aim to identify persons or objects in motion, such as real-time position tracking or patient-flow monitoring to improve workflow in hospitals. In addition, there is track motion via choke points, for example, for access to designated sections. In relation to assets, tracking is applied to inventory location tracking, such as the tracking of availability, maintenance and materials, to prohibit 'left-ins' during surgery: for example, blood products. IoT for identification and authentication focuses on patient identification to decrease incidents of harm to patients from drugs-overdose. In addition, there is comprehensive electronic medical record maintenance for both in-patients and out-patients. Identification and authentication of assets is predominantly applied to meet the requirements of security plans, to prevent thefts or losses of important products and devices. Furthermore, data collection and transfer aims to diminish process automation, such as collection errors and data entry, processing time, procedure auditing and automated care and medical inventory management. With the increased integration of such IoT technologies, users will continue to rely on their availability, i.e. they are available when needed and provide robust healthcare data. The approach to preventing DoS attacks posited in this paper ensures this availability.

MANET has several features due to its nature that expose it to attack (Singh et al., 2014a). For example, there is an absence of administrative points to monitor nodes leading to little or superficial authentication amongst nodes. Attacks in MANET are likely to come from within the network or when networks merge as they have a limited wireless range, which is not a constraint of wired networks (Raj et al., 2015). Besides, the devices forming a MANET, such as IoT sensors, have a limited battery life, making MANET unreliable (Yadav and Sharma, 2015). Moreover, mass data processing caused by attacks place computational load that the device is not designed to handle and will drain power faster than in normal operations. Due to these limitations, MANET is vulnerable to various attacks, such as eavesdropping, masquerading, message fabrication, and denial of service (DoS) attacks. A DoS attack deprives legitimate users of access to the service (Jia et al., 2013). Thus, the network becomes paralysed, reducing network performance drastically. Detecting a DoS attack can be complicated as there are many types, and each type has a different action (Zain et al., 2015).

MANETs underpin IoT infrastructures due to their dynamic topology and mobility; nodes can join and leave the network frequently, introducing the possibility of MANET merging and partitioning and the issues that this creates. There are many points that need to be considered in these situations, including IP configuration, IP conflict and MANET IDs. In addition, DoS attacks could occur when two MANETs are about to merge and a response in such a situation must therefore be considered (Singh et al., 2014b). A smaller network will always be adopted by a larger one and new addresses allocated for the newly formed network. The protocol for this should be efficient and must assign IP addresses without any disruption of ongoing communications.

In order to perform an efficient detection and response to DoS attacks in multiple MANET (MM), the novel Merging Using MrDR (MUMrDR) method is proposed in this paper for the detection of attacks when two MANET merge and are, therefore, vulnerable to misbehaving nodes. A Grayhole attack simulated in NS2 is used as an example of DoS attack to evaluate the MUMrDR method. The proposed method is based on using a trust concept between nodes. Calculating a trust value for each node is based on many factors in the Monitoring, Detection and Response (MrDR) method. It should be noted that this study is the first study dealing with DoS attack detection during MANET mergers. However, the MrDR method has previously been used to detect DoS attacks, such as blackhole attacks, wormhole attacks, grayhole attacks and jellyfish attacks, against a single MANET (SM) (Alsumayt et al., 2015).

This paper is organised as follows: Section 2 presents previous work relevant to the current study. Section 3 identifies the challenges associated with merging MANETs. Section 4 explains the proposed method to assign IP addresses. Section 5 outlines the MUMrDR method, its performance, and assumptions. Section 6 describes the simulation parameters and results of using the proposed method. Section 7 discusses the results of using the proposed method. Finally, we present our conclusions and suggest further work.

2. Related Work

Many studies propose methods to detect DoS attacks in MANET. For example, the use of traditional methods such as firewalls and the Intrusion Detection System (IDS) has been discussed by various researchers for this purpose. Other methods use a trust concept between nodes in MANETs that need IP address configuration in the event of MANET merging. Both traditional and other methods used to detect DoS attacks based on trust concepts are discussed in detail in(Alsumayt and Haggerty, 2014a ; Alsumayt and Haggerty, 2014b). The current section briefly presents a summary of studies that aim to configure IP addresses in the merging scenario and the methods used for misbehaviour detection.

2.1 Assign IP address

Internet Protocol (IP) address configuration is a critical issue in MANET. Due to the mobility and dynamic topology, IP conflict may occur. Methods that are used to configure IP address in other types than MANET such wired networks cannot work successfully in MANET due to its nature. The Dynamic Host Configuration Protocol (DHCP) is a standardised network protocol that is utilised on IP networks to distribute network configuration parameters dynamically, for example, IP addresses for interfaces and services. Devices using DHCP could request networking parameters and IP addresses automatically from a DHCP server. This reduces the need of a user or a network administrator to manually configure these settings (Carrell et al., 2012). However, DHCP could not be used in MANET because it requires a central server to allocate IP addresses to nodes (Choudhury et al., 2015). Three kinds of method are used in assigning IP addresses in MANET: decentralised allocation, leader-based allocation and best effort allocation. Most of these schemes use the Duplicate Address Detection (DAD) method in order to identify IP address conflicts on the network. Using the DAD algorithm when a new node enters to the network, or when MANET merge (Wang and Qian, 2014). For example, the new node gets a temporary IP address and utilises the DAD method to check the availability of this IP address with all other nodes within the network. Then, the node sends a Duplicate Address Probe (DAP) message to nodes and waits to receive the Address Conflict Notice (ACN) message in specific timeout duration. If the ACN is not received, the node assumes that the IP address is available. There are a number of limitations to using the DAD method. First, in the situation that the packet reaches its destination there is a chance that the duplicate is being tolerated. Second, this scheme relies on routing protocols, that involves traffic overhead that is caused by the routing packets (Vaidya, 2002). (Bag et al., 2015)propose a novel address allocation scheme. It is based on simple mutual authentication, so each node is able to generate a unique IP address for any new nodes. Thus, there is no need to use the DAD algorithm, which lowers network overhead significantly. After the allocation process is completed successfully, allocating nodes can broadcast information about the new node. The new node is authenticated by the existing node. Every node in this method has an ID. Besides, a novel solution for both MANET merging and the more complicated scenario as the MANET ID is part of the IP address is the same for the merging MANETs. Granting a unique name for every MANET allow its own group members to be identified from other hosts from different networks. A survey about different methods to assign IP address in MANET is explained in (Amgahd and Yadav, 2016).

2.2 Using trust to detect misbehaving nodes

Distributed Cooperative Trust based Intrusion Detection (DICOTIDS) architecture for MANETs is posited to protect the network from misbehaviour, such as selfish and malicious nodes. The key concept of this framework is to utilise both direct and indirect observations among nodes. Furthermore, this framework targets false trust information broadcasted by malicious nodes within the network. The 'promiscuous mode' is used which can observe other nodes. The main aim of DICOTIDS is to detect misbehaving nodes that propagate false detection alerts in MANET (Mutlu and Yilmaz, 2011). Another multidimensional trust-based outlier detection algorithm has been proposed in (Li et al., 2009). This allows nodes that have exhibited abnormal activities to be identified. Also, this method evaluates the trustworthiness of nodes from three perspectives: Behavioural Trust (BET); Collaboration Trust (COLT); and Reference Trust (RET). This algorithm is better than other methods such as the Simple Averaging (SA) method and Simple trust-based Weighted Voting (SWV). The drawbacks of this method are due to differing circumstances; for instance, when the majority of nodes are malicious, then the local views are unreliable. In addition, this method is overly robust in small communication overheads (Li et al., 2012).Another study poses a survey on trust-based routing protocols in MANET (Thorat and Kulkarni, 2014). Another paper includes a survey about reputation based schemes to compromise misbehaving nodes is discussed in (Abbas et al., 2010). Our previous paper explains the proposed method in detail (Alsumayt et al., 2016) and this current article evaluates the MUMrDR method for the situation when two MANETs are merged.

As explained above, the existing methods have a number of drawbacks. The first is related to the assignment of the IP address in MANET. For instance, the use of the DAD algorithm to assign IP addresses in MANET can lead to extra communication overhead. Thus, this is not appropriate for MANET, which has limited energy. Additionally, in (Bag et al., 2015), it is shown that each node can generate an IP address for a node that requires it, although the study does not discuss security aspects. For example, if the node is malicious, it can give a duplicate IP address to the new node, which can cause IP address conflicts. Second, there are some drawbacks involved in the use of trust concept for misbehaviour detection: for instance, the shortage of a trust factor used to identify the nodes as trusted or malicious (Mutlu and Yilmaz, 2011). However, no studies discuss the detection of DoS attacks in MANET merging. The studies in the literature essentially handle IP address configuration and do not discuss security. Therefore, there is a need to address this situation specifically and this is what the current study aims to achieve.

3. Merging MANETs challenges

Each node in a MANET must have a unique IP address. This is an essential requirement for continued communications between nodes and prevents the collapse of network communications. IP address conflict is the main concern in this scenario. In addition, whether the node leaves the network abruptly or gradually, IP address reclamation is essential as IP addresses should be made available to other, newly joining nodes. When a node leaves the network abruptly, it leads to IP address leak. There are some IP addresses that are neither assigned to any node, nor available for assignment. Moreover, during the few minutes, or even seconds, it takes for two MANETs to merge to become a single network, they would be vulnerable to a DoS attack. Therefore, there should be a mechanism to ensure that the two MANETs are merged securely.

4. The proposed method of IP address configuration

The existing methods to assign IP address to a new node do not meet current requirements, so a new method for assigning the IP address is proposed in this section. The proposed method to assign IP addresses helps nodes in the network to cooperate and assign IP addresses for new nodes or for any node which needs a IP address in situations such as when MANETs merge. As illustrated in Figure 1, node F is a new node which will join the network. Node F broadcasts REQIP (Request IP Address) to its one-hop nodes or immediate nodes (A, B, C) (see 1 in Figure 1). Nodes A, B and C receive this request from node F. When any of these nodes have a vacant IP address, then it would send a REPT (Reply IP Table) that contains only one vacant IP address. However, some nodes might have more than one vacant IP address, but only one will be sent. The REPT is sent as shown in Table 1. The first node which replies would be considered and the others would be discarded. Node F will allocate the IP address and broadcast the confirmation of the allocation to node C (see 3 in Figure 1). Node C broadcasts the allocation to all its immediate nodes A and D (see 4 in

Figure 1). In addition, they broadcast this to their immediate nodes (see 5 in Figure 1) and so on to update their vacant IP address lists (Alsumayt et al., 2016).

5. Using MUMrDR to merge MM

In this article, MUMrDR is used to detect DoS attack when two MANET are merging. In addition, the aforementioned IP address configuration is used, together with MrDR, in order to merge two MANET successfully and securely. In addition, a centralised trust concept is used in this experiment to complete the merging process.

5.1 An overview of MrDR method

There are three main stages of MrDR: Monitoring stage; Detection stage; and Rehabilitation stage. All these stages help to calculate the Total Trust Value (TTSV) of each node.

First, Monitoring stage which aims to monitor the network and detects misbehaving activities whether malicious or selfish nodes as early as possible. Two types of checks are applied in this stage. Accomplishment Trust Value (ATV) that composed from two values: ATV1 and ATV2. ATV1 indicates where the node sends the required packet to the intended destination, then the ATV=0.5, otherwise ATV1=0. ATV2=0.5 when the node sends a confirmation message that determines it has already received the packet. Furthermore, When it fails to send this confirmation, then ATV2=0. The overall calculation of ATV value is as follows:

$$\boldsymbol{ATV = ATV1 + ATV2} \qquad (1)$$

The second stage aims to calculate the Reputation Trust Value (RTV). It is assumed that the punishment attached to packet dropping is more minimal than packet fabrication. The reason for the latter is packet dropping is not always due to the occurrence of misbehaviour. It might occur due to network congestion, faulty device components, or power. Thereupon, the node will have a good reputation if it does not modify packets, drop packets, cause DoS attacks, or misroute packets. If the node drops the packet for first time, then the RTV value for it is 0.5. When the node undertakes it again, the RTV is equal to 0.25. Since the node drops the packet for the third successive time, then the RTV is equal to 0 and the node is considered as a malicious. However, in the situations that the node misroutes packets, modifies packets, or launches a DoS attack, the RTV directly is equal to 0. Otherwise, the RTV=1 in normal behaviour.

Third stage of the proposed method is the Detection stage. The goal of this stage is to detect misbehaving nodes. The Honesty Trust Value (HTV) is calculated in this stage in order to assess the trustworthiness of the nodes or not. When the node exchanges the trust values and that information is matched with the information from the majority of nodes, then the HTV is equal to 1. Otherwise, the HTV=0. Subsequently, the TTSV is calculated as follows:

$$\text{TTSV} = \begin{cases} 0, & ATV < 1\,,\ RTV < 1,\ HTV = 0 \\ 1, & ATV = 1\,,\ RTV = 1,\ HTV = 1 \end{cases} (2)$$

Lastly is the Rehabilitation stage. In this stage, the MANET aims to rehabilitate the misbehaving nodes that could reused in future communication. The dynamic topology of nodes in a MANET emphasise that nodes cannot be in one status all the time. Therefore, the first and second stages would be repeated every (n) seconds depending on the misbehaving rate as is shown in Equation 3:

$$\boldsymbol{CTV} = \frac{\boldsymbol{ETT}}{\mathbf{3}} (3)$$

CTV relates to theCheck Trust Value, whereas ETT refers to the Equation Total Time. For example, in the situation that a node X is being malicious for three successive times, then the rehabilitation would be longer, as demonstrated in Equation 4 below:

$$\boldsymbol{CTV} = \frac{\boldsymbol{ETT}}{\mathbf{2}} (4)$$

Accordingly, it saves the power as the node is definitely malicious. The MrDR method relies upon a trust concept, which is assumed not to be transitive. Trust values in this method are short-lived and temporal, and therefore need to be frequently recalculated due to the non-fixed infrastructure of MANET. Notably, the MrDR method is the first method that uses the trust value as a binary number of trusted=1 and untrusted=0. The proposed method in this study is a centralised control system within a decentralised environment, which monitors nodes and ensures that communications are between trusted nodes and avoid misbehaving nodes, temporarily.

5.2 Grayhole attack

With its various vulnerabilities, including the absence of central authority and dynamic topology, MANET is prone to a number of different attacks. These attacks are applicable as nodes in MANET that are designed to cooperate in order to perform network operations, since MANET does not have grounds for *a priori* classification. The grayhole attack is used in this study as an example of a DoS attack in order to evaluate the proposed method when two MANETs merge. Another reason for using this type of DoS attack as an example in this paper is that a grayhole attack is difficult to detect. This is because conversion between normal and malicious modes can occur frequently. For instance, a grayhole node can drop packets and return to normal mode and then send legitimate packets that make detection more complex.

Sometimes, a grayhole attack is also referred to as 'node misbehaving attack'. In a grayhole attack, a malicious node pretends to be a normal node in order to precede specific packets and simply drops them. The attacker drops the packets selectively, choosing those originating from a range of IP addresses or a single IP address, and forwards the remaining packets (Pokhariyal and Kumar, 2014). The grayhole node exploits the *ad hoc* on-demand distance vector routing (AODV) protocol and announce itself that it has a valid route to the destination node, with the intention of humiliating packets, interjecting, or even though route is fake (Jhaveri et al., 2012).

When the grayhole node receives packets from neighbouring nodes, the attacker drops the packets. The attacking node behaves normally initially and sends true RREP messages in reply to nodes sending RREQ messages. After it receives packets, it starts dropping them. A grayhole node fabricates packets while forwarding them in the network (Lonavala, 2014). Grayhole nodes behave maliciously for some time, until packets are dropped, and then switch back to the normal mode. Figure 2 represents the architecture of this attack in MANETs as node M is the grayhole node which drop packets between the source node S and destination node D. In addition, node M might behave normally sometimes which made the detection harder (Patel and Chawda, 2015).

5.3 Merged Two MANETs Based on centralised trust

This method is based on using a trusted node from each network as a manager. Thus, these nodes are responsible for the allocation of IP addresses to all nodes in their domain in the event of an IP conflict. Moreover, managers must be trusted, in the absence of which they are unable to complete their duties to accomplish the merging process. Consequently, another trusted node would be nominated to complete the merging process.

In Figure 3, C and D are trusted nodes, or *connected nodes*, and their main responsibility is to help the two MANET merge smoothly. Nodes C and D also have some checking duties. First, there must not be any IP address conflicts between nodes within the network. Second, any misbehaving nodes such as malicious or selfish nodes need to perform a rehabilitation process. For instance, in Figure 3, it is now the responsibility of node C, which is such a manager, to check the status of node F and apply rehabilitation to it. Third, managers C and D nodes are responsible to allocate the IP addresses to all nodes in their domain, and identify when any IP address conflicts occur. Furthermore, managers must be trusted otherwise they cannot complete the merging process. Therefore, another trusted node will be nominated to complete the merging process. For example, if node D is untrusted, node C will communicate with other nodes in MANET 2, such as node E. If the node leaves the network, then its IP address will be reclaimed. Thus, the immediate node will maintain this vacant IP address until it is needed. The complete explanation of this concept is detailed in (Alsumayt et al., 2016).

6. Simulation

An experimental investigation is conducted to demonstrate the applicability of the MrDR method in detecting DoS attacks in MM. As described above, a grayhole attack is used as an example of DoS attack in order to test the performance of the proposed method. The Network Simulator (NS2.35) is used to perform this experiment under Linux (Ubuntu 12.04). This section illustrates the simulation parameters, experiment scenario, and the results.

6.1 Simulation parameters

Table 2 outlines the computer specifications and simulation parameters that are used in this experiment.

6.2 Experimental design and results

In this experiment two MANETs are used. The first MANET – MANET 1 – comprises 71 nodes. Figure 4 shows the architecture of MANET 1.

In this experiment, it is assumed that the source node is node 8 and the destination node is node 7. Moreover, it is also assumed that the majority of nodes are normal nodes. Figure 5 shows the timeline of the experiment and the scenario of each stage.

The network performance is verified three times prior to the pre-merging stage and three times at the post-merging stage. However, in a real-world deployment of the system, this verification is an iterative process. Three scenarios are examined at each stage: before the attack occurs; when the attack occurs; and subsequent to removing the attack from the communications. Three factors are measured in each scenario: packet delivery ratio; network throughput; and packet delay ratio. According to Figure 6, normal network mode or when no attack has occurred, signifies the network performance is positive. In technical terms, the network throughput and packet delivery ratio is high, and the packet delay ratio is low. The reason for this is the absence of any attacks that can hinder the network performance.

In reference to Figure 5in the attack phase, two grayhole nodes occur in node 10 and node 18 (Figure 7, A). Further, at the beginning of minute three, two extra grayhole attacks subsequently occur in nodes 16 and 25 (Figure 7, B).

The network performance is measured simultaneously with the occurrence of the malicious nodes, as shown in Figure 8. Grayhole nodes harm the network and affect network communications. As the grayhole attacks deteriorate the network communications, the network throughput and packet delivery ratio decreases, whereas the packet delay ratio and network overhead increases.

At the mid-point of minute four or the detection phase based on Figure 5, grayhole nodes 10 and 18 are removed gradually using the proposed method. In Figure 9(A), node 10 and node 18 are detected and isolated temporarily from the communication using the MrDR method. At the termination of minute four, nodes 16 and 26 are also detected using the proposed method and isolated until their trusted value increases from 0 to 1 (Figure 9, B). Figure 10 shows the network performance subsequent to the detection of grayhole attacks. As the grayhole attacks are detected using the proposed method, the network throughput and packet delivery ratio increases again, whereas the network overhead and packet delay ratio decreases rapidly.

Moreover, Figure (9, B) demonstrates that a novel MANET – MANET 2 – is on the point of merging with MANET 1. MANET 2 is composed of 30 nodes and merged with MANET 1 to form a single entity and a larger MANET based on a centralised trust concept, which is explained in sub-section 5.3. A trusted node from each MANET facilitates in the accomplishment of the process and finalises the merging between the two networks. In this experiment, node 5 from MANET 1 and node 85 from MANET 2 are the connected nodes that possess the responsibility for completing the merging operation and checking the IP address for conflict of each node.

Furthermore, nodes 16 and 25 are also detected using this proposed method however at the mid-point of minute five (Figure 5). After the negations between the two networks, the merging process commences, until the MANET are unified as illustrated in Figure 5. After merging at the beginning of minute six, the MANET comprises 101 nodes as shown in Figure 11(A and B). Figure 12 shows the network performance for this large MANET, demonstrating the lack of DoS attacks. The network throughput and packet delivery ratio increase, whereas the packet delay ratio decreases. Then, 30 seconds post-merging or the attack phase in Figure 5, grayhole attacks occur in nodes 12 and 39, as shown in Figure 13.

In addition, the network performance during this attack is shown in Figure 14. For network performance in this situation the network throughput and packet delivery ratio decreases, but packet delay ratio and network overhead increases considerably. This is evidently attributed to the occurrence of the grayhole attack, which degrades the network performance significantly.

At the mid-point of minute six or in the detection mode based on Figure 5, these malicious nodes are detected progressively using the proposed method. Figure 15 illustrates the network performance after grayhole attacks are resolved. The packet delivery ratio and network throughput increase, but the packet delay ratio and network overhead decrease. The normality of the network performance stems from the comprehensive detection of the grayhole attacks, considering there are no hindrances that affect the communications.

7. Discussion

MANET, with its dynamic topology, mobility and lack of fixed infrastructure, is prone to attacks such as DoS. According to the high mobility of a MANET's nodes, the likelihood of MANET merging is a distinct possibility. However, studies discussing this situation specifically are lacking. In order to ensure that MANET merging is safe and also to detect any DoS attacks in this critical scenario, the MrDR method is proposed. For this experiment, grayhole attack is used as an example of DoS attack to evaluate and test the efficacy of the MrDR method against this type of DoS attack.

MrDR is used to detect DoS attacks when two MANET merge. Assigning an IP address to new nodes, checking for IP address conflict, reclamation of IP addresses, and MANET IDs, are all aspects that need to be considered when MANET merge. The proposed method in this experiment, using the centralised trust concept, utilises trusted nodes within each MANET to facilitate the merging process. Trusted nodes, or the connected nodes in each MANET, are responsible for accomplishing MANET mergers. The centralised trust concept is used in this experiment to check any IP address conflicts and to fulfil the merging process, based on the MrDR method. These processes need to be completed rapidly, in order to prevent any conflict between nodes. These negotiations that only trusted nodes facilitate merging, and information from untrusted nodes is isolated temporarily. Subsequently, the trust value of each node will be recalculated, as previously explained. Trust value only two values: trusted=1 and untrusted=0. The trust values are short-lived and so need to be recalculated frequently.

Rehabilitation occurs for each node as the trust value is tested frequently. All nodes that are untrusted for three successive attempts will be isolated from communications for increasing lengths of time, such as 180 seconds (Equation 4). However, in order to measure the network performance before and after merging, the trust value for each node will be recalculated three times pre-merging and three times post-merging.

A grayhole attack is used in this experiment to evaluate the proposed method pre- and post-merging. Many aspects are considered, such as network throughput, packet delivery ratio, and packet delay ratio. In addition, network overhead is also measured, to check whether this factor is affected by the proposed method. These measurements are calculated pre-merging and post-merging as shown in Figure 5 which illustrates the experiment scenario. The results in Figure 10 and Figure 15 show that the network overhead does not increase in response to using this approach; it is only affected when a grayhole attack occurs, as shown in Figure 8 and Figure 14. Moreover, the network performance after detecting grayhole attacks using the proposed method emphasise the performance of the proposed method as shown in Figure 10 and Figure 15.

As demonstrated above, the possibility of DoS attacks occurring when MANET merge is potentially acute due to the issue of two (or more) networks of untrusted nodes joining together. However, to the authors' knowledge, this is the first study to identify this issue and propose an approach for its mitigation.

8. Conclusion and Future work

MANET is a system of freely mobile nodes that communicate with each other, however, it is vulnerable to attack. In this study MrDR is used to test the efficacy of this method when two MANET are merging. This scenario is critical, as many points need to be considered, such as IP configuration, conflicting IP addresses, and MANET IDs. In this paper, we tested the proposed method against grayhole attacks when two MANETs merge. The proposed method is based on using a trust concept and measuring the trust value for each node to detect the DoS attack. In addition, trusted nodes will help to accomplish the merging process in each MANET. A centralised concept is used in this experiment as trusted nodes in each MANET, which are called connected nodes, will help to merge MANETs. The simulation results determine that the proposed method helps to detect this attack successfully.

This work could be extended to employing this technique against different kinds of DoS attack. Moreover, this study uses a centralised trust concept. In future, a decentralised trust concept will be tested to assign IP addresses when more than two MANETs are merging, with different types of DoS attacks occurring simultaneously. For example, when four MANETs are merging and several types of DoS attacks occur, such as a wormhole attack, blackhole attack, and jellyfish attack. The decentralised trust concept means that every node from MANET 1 will communicate with MANET 2 to fulfil the merging process completely and assign IP addresses when conflicts occur. However, nodes whether trusted or untrusted will cooperate to complete the merging the process. This differs from the centralised concept, which nominates one trusted node in each MANET to complete the merging process. In the decentralised concept, all nodes communicate with all other nodes in each MANET to complete the merging process. Finally, nodes in each MANET will help to assign IP addresses, check and compare the trust values, and make the decision to complete the merging process. It is noteworthy that even untrusted nodes cooperate in this situation. This is attributed to the fact that certain DoS attacks, such as grayhole attacks, do not behave maliciously incessantly and can convert to normal mode on occasion. However, if the node gives incorrect information, such as false vacant IP address, then it is isolated from the process until it is deemed trusted or the merging process is complete.

References

ABBAS, S., MERABTI, M. & LLEWELLYN-JONES, D. A Survey of Reputation Based Schemes for MANET. The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, 2010. 21-22.

ALSUMAYT, A. & HAGGERTY, J. A survey of the mitigation methods against DoS attacks on MANETs. Science and Information Conference (SAI), 2014, 27-29 Aug. 2014 2014a. 538-544.

ALSUMAYT, A. & HAGGERTY, J. 2014b. *A Taxonomy of Defence Mechanisms to Mitigate DoS Attacks in MANETs* [Online]. Plymouth University Tenth International Network Conference (INC 2014).

ALSUMAYT, A., HAGGERTY, J. & LOTFI, A. Comparison of the MrDR method against different DoS attacks in MANETs. Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on, 2015. IEEE, 219-224.

ALSUMAYT, A., HAGGERTY, J. & LOTFI, A. Detect DoS Attack Using MrDR Method in Merging Two MANETs. 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 23-25 March 2016 2016. 889-895.

AMGAHD, Y. A. & YADAV, R. 2016. Survey of Mobile IP Protocols.

BABU, B. S., SRIKANTH, K., RAMANJANEYULU, T. & NARAYANA, I. L. 2016. IoT for Healthcare. *International Journal of Science and Research,* 5.

BAG, P., MAJUMDER, K. & DE, D. 2015. A Novel Distributed Dynamic IP Configuration Scheme for MANET. *Intelligent Computing, Communication and Devices.* Springer.

BELLAVISTA, P., CARDONE, G., CORRADI, A. & FOSCHINI, L. 2013. Convergence of MANET and WSN in IoT urban scenarios. *Sensors Journal, IEEE,* 13**,** 3558-3567.

CARRELL, J., CHAPPELL, L., TITTEL, E. & PYLES, J. 2012. *Guide to TCP/IP*, Cengage Learning.

CHOUDHURY, P., MAJUMDER, K. & DE, D. 2015. Secure and Dynamic IP Address Configuration Scheme in MANET. *Intelligent Computing, Communication and Devices.* Springer.

JAIN, R. & GARG, S. 2013. SECURITY GOALS OF MANETs ALONG WITH RESEARCH CHALLENGES & ISSUES.

JAIN, S. 2014. Security Threats in MANETS: A Review. *arXiv preprint arXiv:1405.5320.*

JHAVERI, R. H., PATEL, S. J. & JINWALA, D. C. A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, 2012. IEEE, 556-560.

JIA, Q., SUN, K. & STAVROU, A. 2013. Capability-Based Defenses Against DoS Attacks in Multi-path MANET Communications. *Wireless personal communications,* 73**,** 127-148.

KULKARNI, A. & SATHE, S. 2014. Healthcare applications of the Internet of Things: A Review. *International Journal of Computer Science and Information Technologies,* 5**,** 6229-32.

LI, W., PARKER, J. & JOSHI, A. 2009. Security through collaboration in manets. *Collaborative Computing: Networking, Applications and Worksharing.* Springer.

LI, W., PARKER, J. & JOSHI, A. 2012. Security through collaboration and trust in manets. *Mobile Networks and Applications,* 17**,** 342-352.

LONAVALA, M. I. 2014. A Survey on Security Vulnerabilities And Its CountermeasuresAt Network Layer In MANET.

MUTLU, S. & YILMAZ, G. 2011. A distributed cooperative trust based intrusion detection framework for MANETs. *ICNS,* 11**,** 292-298.

PATEL, A. D. & CHAWDA, K. 2015. Dual security against grayhole attack in MANETs. *Intelligent computing, communication and devices.* Springer.

PATIL, C. S. & PAWAR, K. N. 2016. A Review On: Protocols and Standards in Different Application Areas of IOT.

POKHARIYAL, S. & KUMAR, P. 2014. A Novel Scheme for Detection and Elimination of Blackhole/Grayhole Attack in Manets. *International Journal of Computer Science and Mobile Computing,* 3**,** 217-223.

RAJ, N., BHARTI, P. & THAKUR, S. Vulnerabilities, Challenges and Threats in Securing Mobile Ad-Hoc Network. Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on, 2015. IEEE, 771-775.

SINGH, M., SARANGAL, M. & SINGH, G. 2014a. Review of MANET: Applications & Challenges. *Networking and Communication Engineering,* 6**,** 193-197.

SINGH, S., RAJPAL, N. & SHARMA, A. 2014b. Address allocation for MANET merge and partition using cluster based routing. *SpringerPlus,* 3**,** 1-13.

THORAT, S. & KULKARNI, P. Design issues in trust based routing for MANET. Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on, 2014. IEEE, 1-7.

VAIDYA, N. H. Weak duplicate address detection in mobile ad hoc networks. Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002. ACM, 206-216.

WANG, X. & QIAN, H. 2014. A Distributed Address Configuration Scheme for a MANET. *Journal of Network and Systems Management,* 22**,** 559-582.

YADAV, N. & SHARMA, D. 2015. MANET: Mobile Ad-hoc Network its Characteristics, Challenges, Application and Security Attacks.

ZAIN, A., EL-KHOBBY, H., ELKADER, H. M. A. & ABDELNABY, M. 2015. MANETs performance analysis with dos attack at different routing protocols. *International Journal of Engineering & Technology,* 4**,** 390-398.

List of Figures

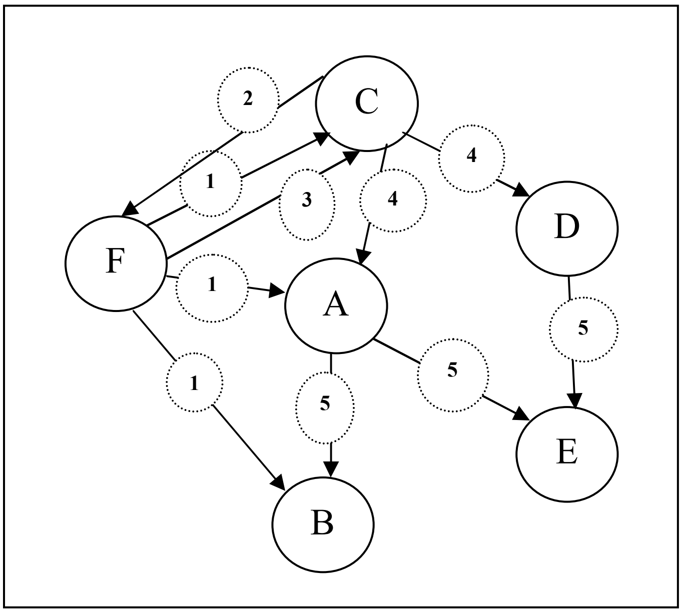

Figure 1. IP address configuration.

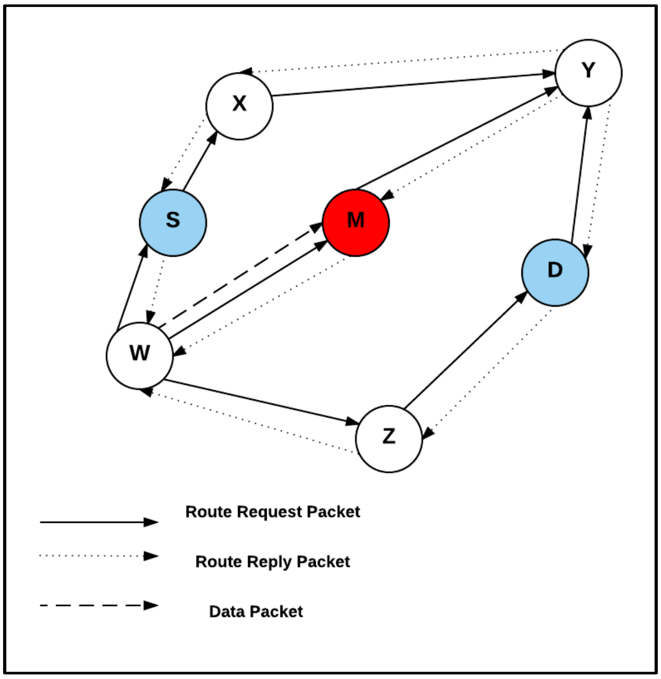

Figure 2. Grayhole attack architecture.

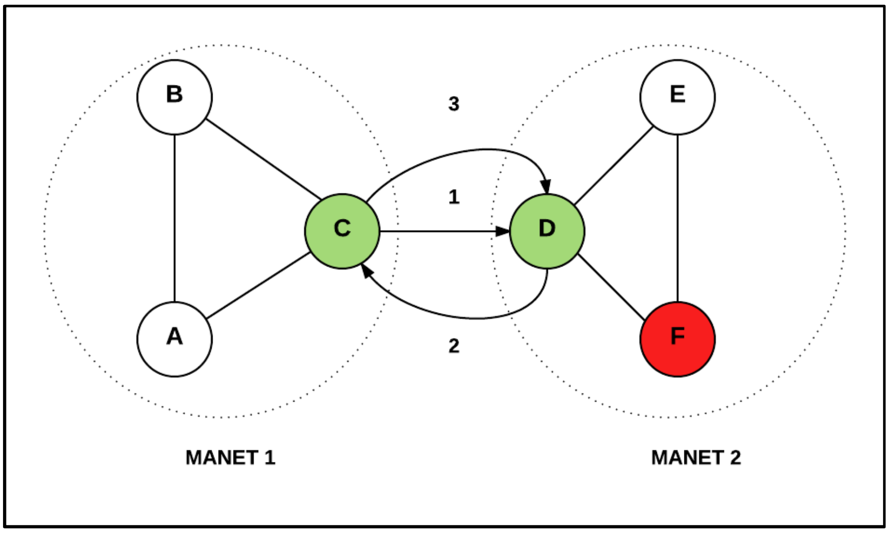

Figure 3. Centralised trust concept.

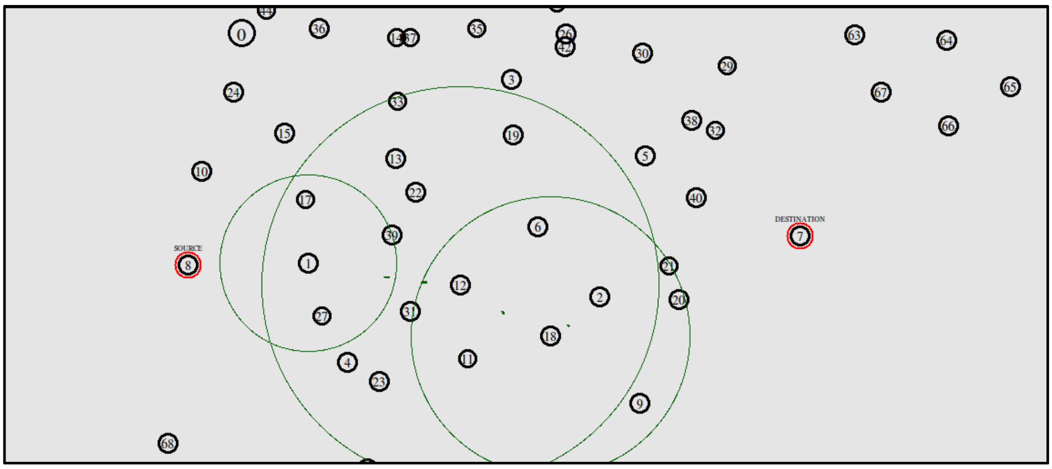

Figure 4.MANET 1 architecture.

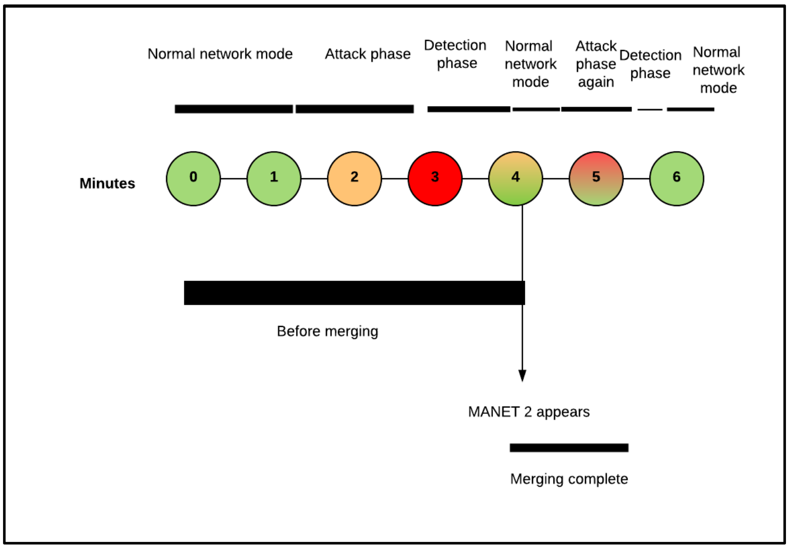

Figure 5.Timeline of the experiment scenario.

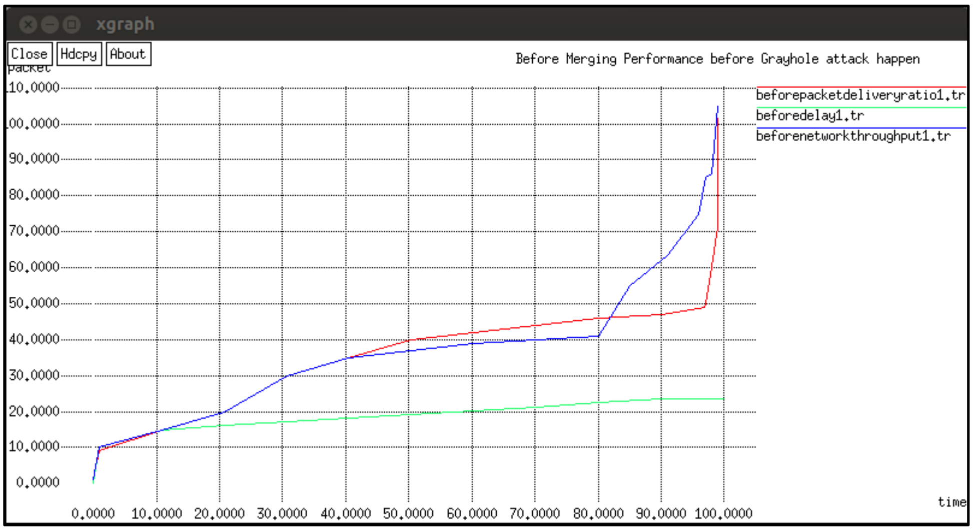

Figure 6. Network performance before the occurrence of grayhole attack (Pre-merging).

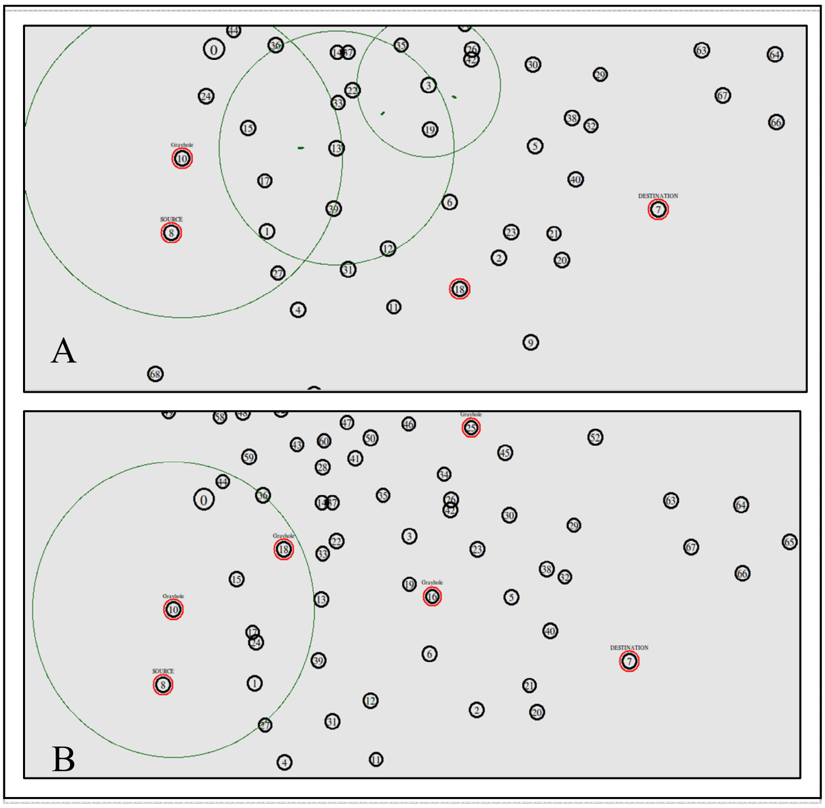

Figure 7. Network architecture following grayhole attacks (pre-merging).

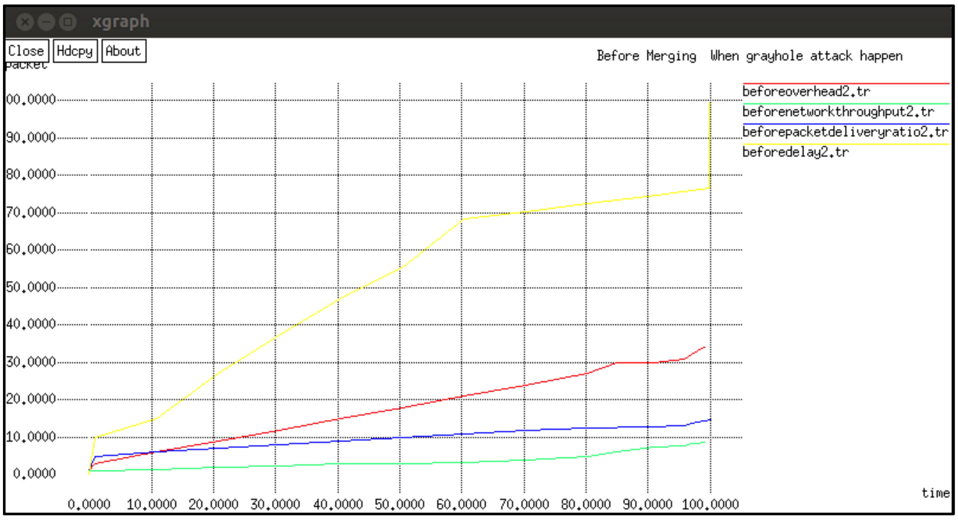

Figure 8. Network performance during grayhole attacks (pre-merging).

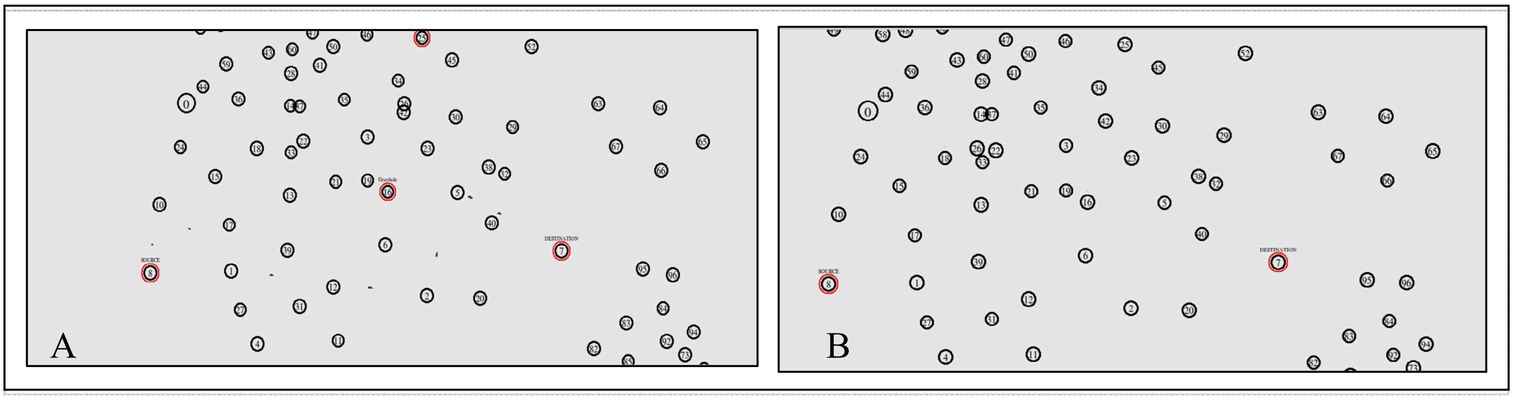

Figure 9. Detection of grayhole attacks gradually (pre-merging).

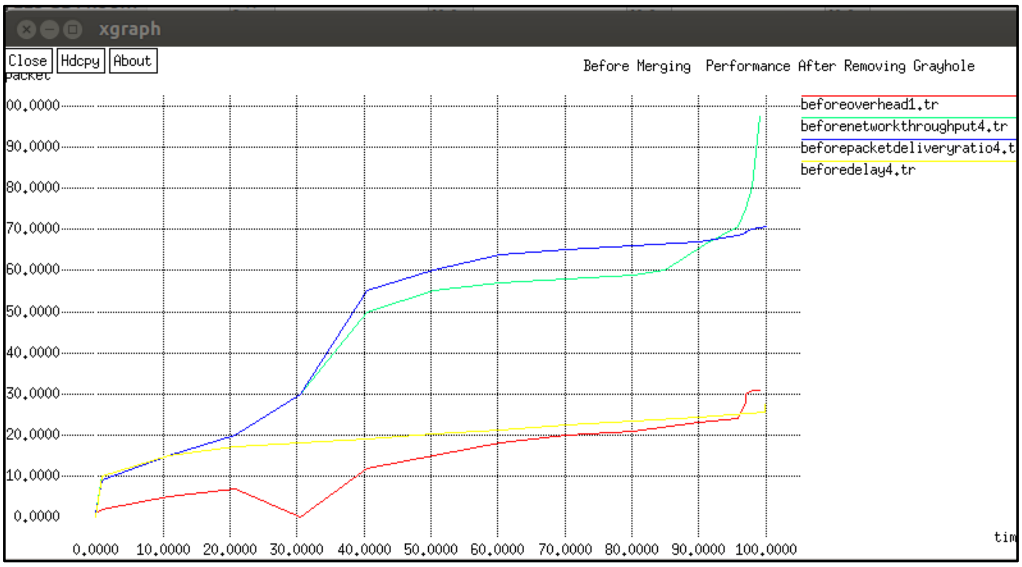

Figure 10. Network performance after removing grayhole attacks (pre-merging).

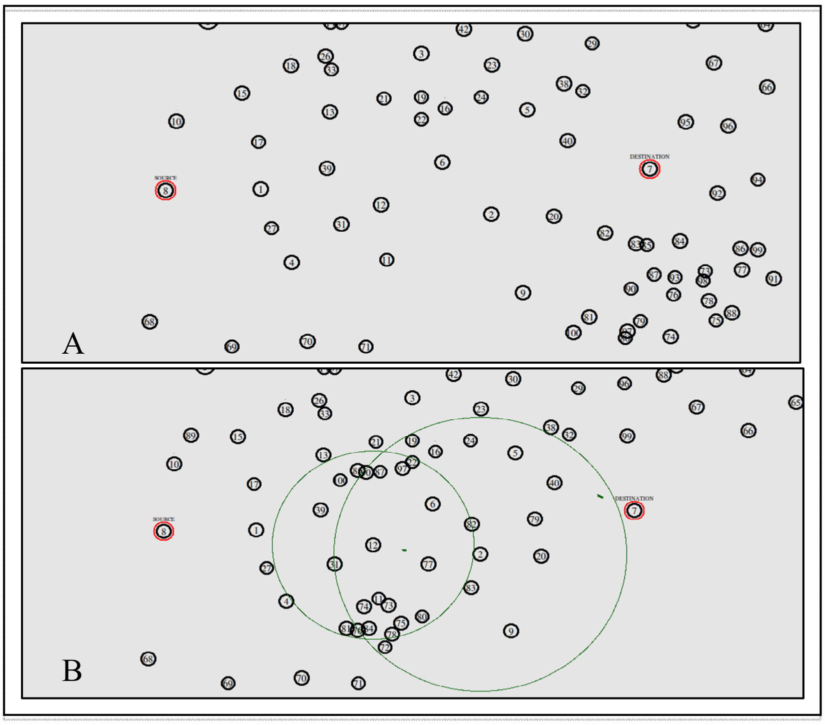

Figure 11. Two MANETs merge.

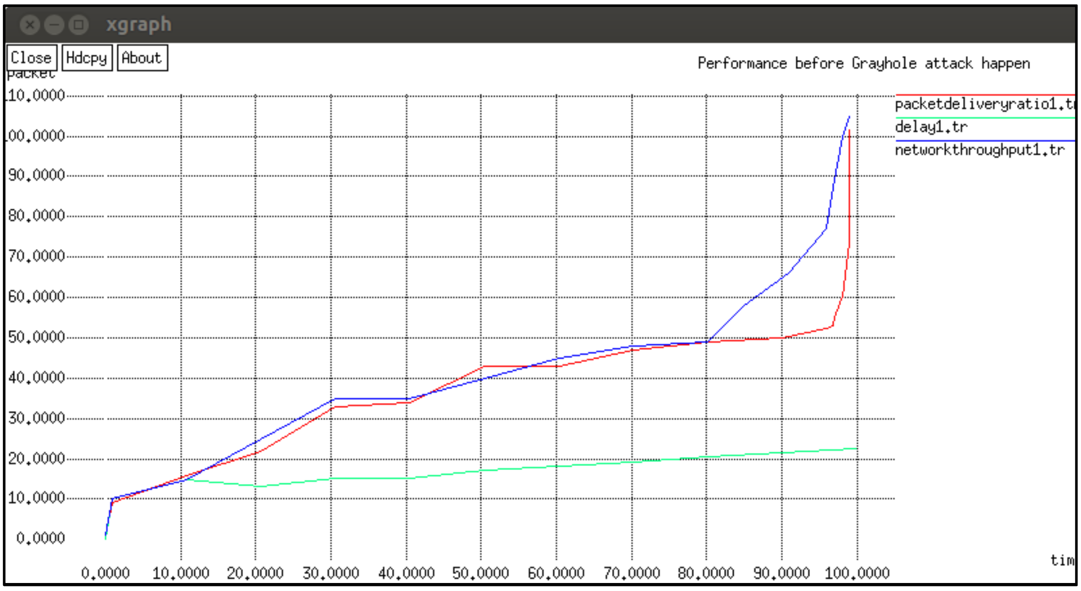

Figure 12. Network performance post-merging and before DoS attacks.

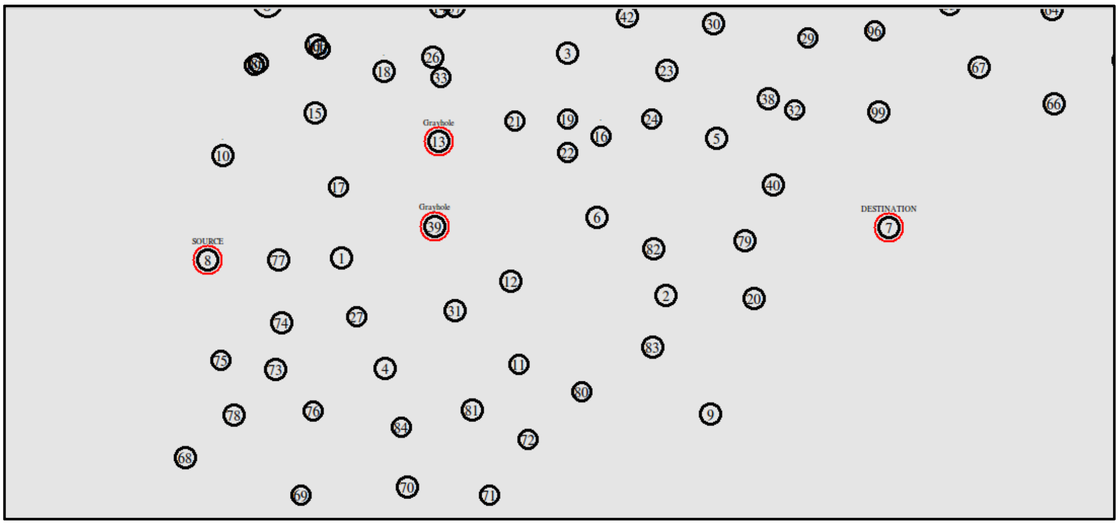

Figure 13.Grayhole attacks (post-merging).

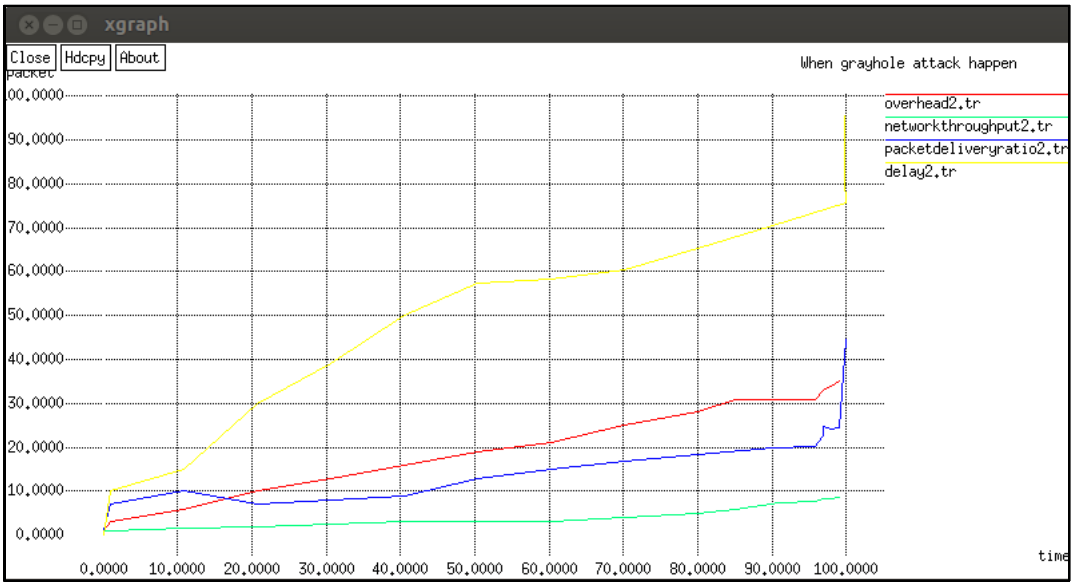

Figure 14. Network performance during grayhole attacks (post-merging).

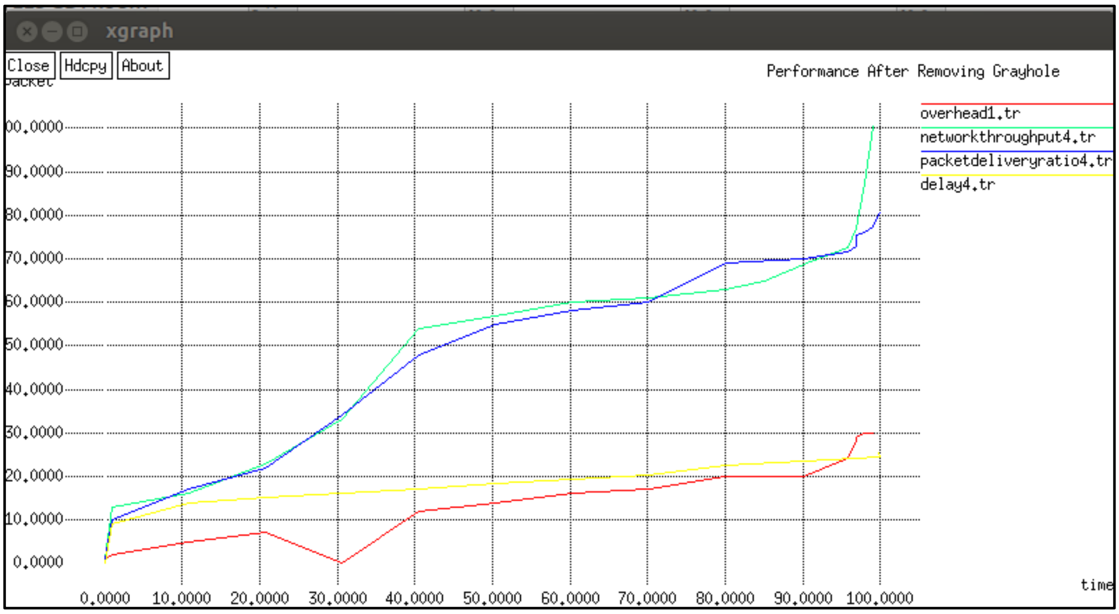

Figure 15. Network performance after removing grayhole attacks (post-merging).

List of Tables

Table 1: Information included in REPT.

Node name	**Vacant IP addresses**
C	196.168.1.2

Table 2. Simulation parameters.

Simulation Parameters	
Processor	Intel(R) Core (TM) Duo CPU P8700 @ 2.53GHz
RAM	4.00 GB
System type	64-bit
Operating system	UBUNTU 12.04
Routing protocol	AODV
Simulation time	6 minutes
No of nodes	101
Traffic type	CBR