2017

A framework for forensic reconstruction of spontaneous ad hoc networks

Alastair Nisbet
Security & Forensic Research Group, Auckland University of Technology, alastair.nisbet@aut.ac.nz

DOI: 10.4225/75/5a8395e11d281

A FRAMEWORK FOR FORENSIC RECONSTRUCTION OF SPONTANEOUS AD HOC NETWORKS

Alastair Nisbet
Security & Forensics Research Group, Information Technology & Software Engineering Department
Auckland University of Technology, Auckland, New Zealand
anisbet@aut.ac.nz

Abstract

Spontaneous ad hoc networks are distinguished by rapid deployment for a specific purpose, with no forward planning or pre-design in their topology. Often these networks will spring up through necessity whenever a network is required urgently but briefly. This may be in a disaster recovery setting, military uses where often the network is unplanned but the devices are pre-installed with security settings, educational networks or networks created as a one-off for a meeting such as in a business organisation. Generally, wireless networks pose problems for forensic investigators because of the open nature of the medium, but if logging procedures and pre-planned connections are in place, past messages, including nefarious activity can often be easily traced through normal forensic practices. However, the often urgent nature of the spontaneous ad hoc communication requirements of these networks leads to the acceptance onto the network of anyone with a wireless device. Additionally, the identity of the network members, their location and the numbers within the network are all unknown. With no centre of control of the network, such as a central server or wireless access point, the ability to forensically reconstruct the network topology and trace a malicious message or other inappropriate or criminal activity would seem impossible. This research aims to demonstrate that forensic reconstruction is possible in these types of networks and the current research provides initial results for how forensic investigators can best undertake these investigations.

Keywords: spontaneous, wireless, wifi, MANET, simulation, forensic investigations

INTRODUCTION

With the introduction in 1997 of the original IEEE 802.11 wireless networking standard, wireless communication 'came of age'. Whilst other, more basic attempts at wireless networking had been developed, the IEEE suite of standards that sprang from the original 2Mbps standard has seen steady advances in throughput, security and usability. Whilst originally envisaged as extensions to existing wired networks by utilising wireless access points, a distinct type of network that departed from using access points was quickly developed. This ad hoc mode allowed users of often mobile devices to connect directly to one another's devices to form a mesh network that could be used in a truly peer to peer fashion. The main advantage was the ability to quickly connect to each other's devices without the need for a preconfigured access point to act as the centre of control for the network (Kuo, Chu 2016). The rapid deployment of ad hoc networks meant that not only pre-planned networks with pre-configured devices could form this topology, but that unplanned networks could also be created on-the-fly for a very specific and often urgent need (Nelson, Steckler et al. 2011). This gives great potential to this type of truly ad hoc network, often referred to as spontaneous networks, but as yet this potential remains largely untapped. With concerns over security, especially with unplanned networks which may allow any person with a device to connect without the need for authorisation or authentication, these networks are used rarely. However, in the past few years the benefits of quick and unplanned network formation are being discussed and security implementations are proposed that have the potential to make even totally unplanned networks have robust security (Lacuesta, Lloret et al. 2013).

One area that has been left out of these discussions and proposed security protocols is that of forensic reconstructions of the networks to trace misbehaving devices. Forensics plays a vital part in seeing the potential of computers and networks utilised because it allows misbehaviour to have a consequence, that of identifying the nefarious device and user and bringing them to account for their behaviour. This research examines the issue of forensic reconstruction of spontaneous ad hoc networks and introduces unique research into how forensic investigators can use techniques which will allow them to trace the origins of misbehaviour back to the originating device. Initial results are discussed and a guide as to how these techniques will be further developed to provide practical implementations of forensic investigations are made.

STATE OF THE ART

On the 14th of September 1999, the two extensions to the original standard provided a security protocol built into the standard which was seen as a significant step forward in acceptance of wireless networking. The 802.11a and 802.11b protocols also greatly increased the throughput from a maximum of 2Mbps to 54Mbps and 11Mbps respectively (IEEE 1999). Whilst the security in the form of WEP proved to have serious flaws which would later be rectified in the form of WPA and WPA2, the increased bandwidth had an immediate and significant effect (Cam-Winget, Housley et al. 2003). Not only did it provide much increased packet throughput, often greater than what was being provided on the LAN at the time, but it meant that an ad hoc networking topology was much more usable (Wang, Wang et al. 2005). This is because in a mesh network, there are often devices communicating at the same time in pairs and within the radio range of other communicating devices. The high bandwidth meant multiple message passing could be carried out with an acceptable bandwidth, even with the interference caused to each other's radio signals. Later, bandwidth would be significantly increased in later revisions to the standard so that today we enjoy bandwidths up to 150Mbps or more in ad hoc networking mode (IEEE 2009). The increasing acceptance of mesh networking, including unplanned spontaneous networks has seen increased awareness of security issues, especially in the form of cryptography with the associated encryption key management challenges. Whilst these are being overcome as new ideas lead to improved protocols, the forensics of spontaneous networks has largely been ignored.

Digital forensics traditionally utilises a life cycle of 4 phases (NIST 2006). These phases are shown in figure 1.

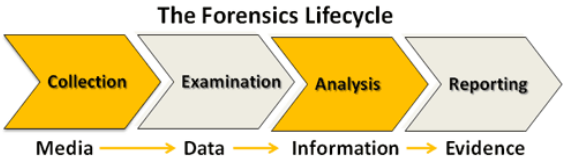

Figure 1: The Digital Forensic Life Cycle

The phases begin by seizing a device, often a computer but possibly other hardware such as a router, switch or wireless access point. In many cases these devices will have logs that will record much of the network traffic that has passed through the device. Whilst configuration of the devices may not include collecting all packets, source and destination address and often some identifying packet information such as headers may be recorded. This can be invaluable information for a forensic investigator who may be building a case against a misbehaving user such as an errant employee in a company or an outsider intruding into a company network. Serious offences may be committed with unauthorised access, use of resources or destruction of data. Many of the offences relating to computer crimes are now contained in New Zealand's Crimes Amendment Act 2003 and include harsh penalties for such behaviour. Most other countries have similar legislation with harsh penalties including long prison terms.

However, the investigation often relies on the ability to seize the offending device and perform an acquisition and analysis of the evidence on this device. Whilst monitoring network traffic may be possible in wired networks, this is not practical in a spontaneous wireless network (N. Malik, J Chandramouli et al. 2017). Network logs, if they exist on the device, may point to the errant device and provide corroborating evidence of the misbehaviour. However, in spontaneous networks where network deployment has no prior planning and often no prior notice of its formation, this first step may prove to be impossible. This is because the users of the network are usually not identified, their devices are not registered for use on the network, their location may change as they move around the network and they may come and go as mobile devices are shut down to save battery power and restarted later to join the network multiple times. Additionally, a node that may be monitoring traffic has a radio range of approximately 300 metres and therefore may be out of range of most of the network. If misbehaviour is detected, there may be the ability to eject a device from the network by revoking a digital certificate (Nisbet, 2014), but attempting to physically locate the device to perform a forensic examination may be unsuccessful (Zhang, Lee et al. 2003). This could be especially true if the user of the device is aware that their device is being sought.

What is required is a method of reconstructing the network at a particular time in its life so that the forensic reconstruction can be performed, possibly without access to the offending device. This research demonstrates through simulation that this type of reconstruction may be possible provided some of the devices in the network can be examined. Additionally, the type and amount of information that can be realistically logged onto the devices is discussed so that an initial guideline can be made as to what percentage of devices in the network are needed to be examined given these varying parameters. The following section discusses the challenges inherent

in forensic evidence gathering from spontaneous network deployment, especially when evidence may be required long after the network has served its purpose and disbanded.

FORENSIC RECONSTRUCTION

In a truly ad hoc network, a mesh network will often form where many of the devices in the network, referred to as nodes, will have one or more neighbours within direct communication distance. This not only allows neighbours to communicate directly with each other, but they can often be used as hopping points for messages to greatly increase the distance of the network communication from the usual 300 metres radio range, to in theory unlimited distances (Nisbet and Rashid 2009). One other benefit of multiple neighbours is that the path utilised to send a message can have many different possible paths from sender to receiver (Suzuki, Kaneko et al. 2006). This redundancy of routes greatly increases the efficiency of message passing and is one significant benefit of mesh networks, but when these networks have at least some nodes that are mobile, the message paths may also change rapidly. This requires a very efficient reactive routing protocol that will find a path through multiple hopping points from sender to receiver, often in both directions if a reply is given as the same route back to the sender may not exist by the time the message is received. This means that routes are changing rapidly as are neighbours and often locations of nodes. This all adds to the considerable complexity of these types of networks and the forensic challenges that stem from these temporal and spatial changes (Dewald 2015).

The current research is in the development phase of initial testing through simulations. A wireless network simulator was constructed utilising Matlab and has been modified to permit nodes in the network to record certain parameters which can then be called upon to attempt to rebuild the network. The process involves deployment of an ad hoc network where the nodes are placed at random on a grid and the network grows as time passes. This simulates the spontaneous deployment of an ad hoc network for any purpose where people have begun communicating with neighbours. Whilst the purpose of deployment of the network is unimportant, it could be for such urgent and unplanned reasons such as when a major disaster has struck knocking out communications or some similar event that requires wireless communication by masses of devices (Shimoda and Gyoda 2011). The network grows as more and more people joint the networks, with some leaving the network temporarily, perhaps to save battery power on their devices, and others joining at apparent random points on the grid. During the time the simulated network is ‘live’, nodes will appear at random points with some nodes mobile and some shutting down temporarily or permanently.

The network simulation runs for a simulation time of 10 minutes which is sufficient with the growth to mimic perhaps several hours in real time. During this time, information is recorded on each node as to its current status, location and the source and destination of any messages that it may send, pass on or receive. One issue here is that recording of information may be desirable but with limited time to record data and limited storage available on many devices, it is necessary to store as little information as is necessary. Therefore, the simulation utilises the ability to call only some or all of the information recorded. This parameter will allow comparisons to be made as to what information is necessary and what difference not having some information will make to the success of a reconstruction. The information recorded in the nodes is shown in table 1.

Table 1: Information recorded in the nodes

Attribute	Format
Live	yes / no
Neighbours	node IDs
Neighbour Location	x and y coordinates
Server	yes / no
Network Number	integer
Position	x and y coordinates

Once the simulation has completed, a time from 1 second to the end of the simulation is selected to attempt the reconstruction. This time represents when a malicious act has occurred and the offending node needs to be identified. For example, this may be an act such as a false message about rescue in a disaster area that may have led to serious injury or death. Each node records the information shown in table 1, along with other information related to security settings. It is unlikely that all devices that were in the network can be recovered. Here, a distinction needs to be drawn as to which devices qualify. Either it can be those devices that were live at the time the misbehaviour occurred or alternatively all devices that have ever appeared in the network. A call to those people who may have participated in the network may results in devices that were not live at the time of the misbehaviour and for this reason the reconstructions have chosen to include these ‘no longer live’ nodes. The

reconstruction of the networks begins with a variable parameter of what percentage of nodes were able to be recovered for examination. This could range from one device to all devices. Figure 1 shows a network that has grown over a period of 60 seconds and now contains a total of 24 nodes. What is interesting to note is that rather than a single network forming, 3 separate networks have formed independently. Of these, only the biggest network has reached a capacity where digital certificates can be issued, shown by the red labels on the nodes. The nodes out of 300 metre range of another node are shown isolated with a circle representing the 300 metre radio range. The 2 small networks at the bottom of the grid have 2 members each. This snapshot of the network is taken during the live network simulation. The goal is therefore to reconstruct the network well after the network has ceased and the nodes have disbanded. This must be achieved as accurately as possible so that nodes in the network can be identified and placed in their location at any chosen time, such as when a malicious message was sent.

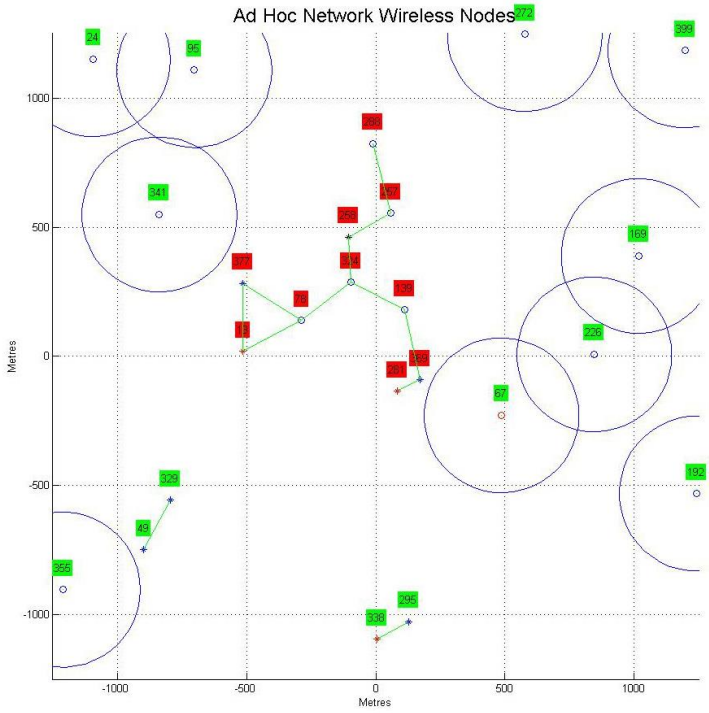

Figure 2: Spontaneous network at 60 seconds

One challenge that is immediately apparent is that whilst the goal may be to identify a misbehaving node in a network, there is no record of the members of the network until devices that participated in the network have been examined (Graffi, Mogre et al. 2007). This leads to 2 desirable records that could be stored dynamically that would greatly assist the forensic investigator to reconstruct the network and trace the origin of the malicious message. The first is to identify and collect at least 1 member of the target network. The second is to have a record of all members who were in the network at the time recorded in every device in the network. This would mean that collecting any single device would give all information about the identities of all devices in the network. Here, identities simply refer to a unique identifier for the device but this would not include who was using the device. Additionally, the unique identifier, at least for the lifetime of the network, and the location of the device at the chosen time would not disclose any private information relating to the user of the device.

This is an example of what would be most desirable and could be written into a protocol with forensic readiness in mind when designing the protocol. Without this preparedness, the investigator would need to collect as many devices as possible, possibly through advertising for network participants, and then analyse the devices initially to determine if they had belonged to the relevant network at the time of the offence. With the ability to store relevant forensic evidence within each of the network members' devices, the network can be reconstructed by looking through the evidence of each collected node and placing nodes in the network space as they were at the chosen time. An example of this is 2 views of the network reconstructed in this manner and shown in figure 3.

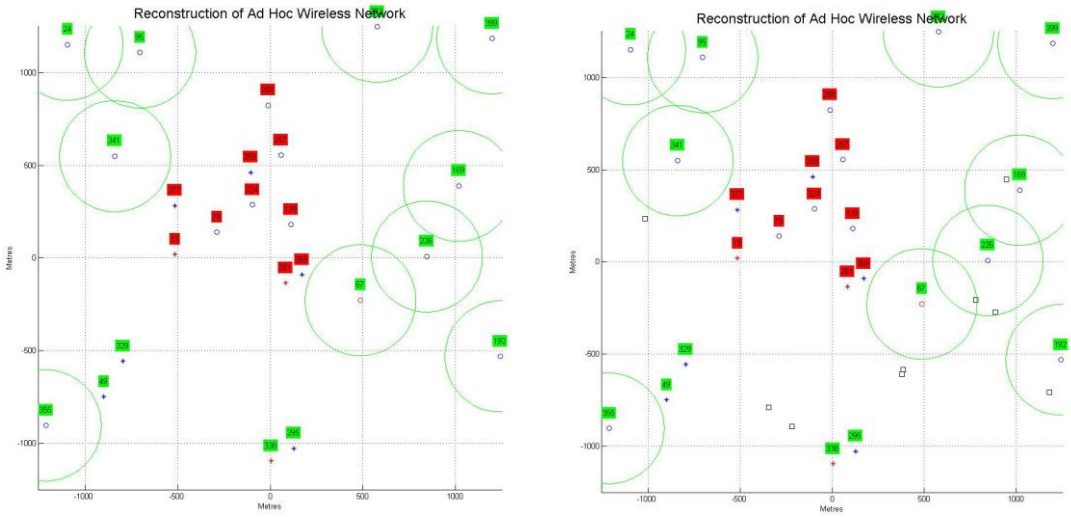

Figure 3: Reconstruction of the network at 60 seconds

A comparison with figure 2 shows that the reconstruction is successful. The target time is 60 seconds after the formation of the network, and this could represent a specific time when a malicious message was sent leading to serious consequences. The left side of this figure shows only those nodes that were live at the tick of the clock of 60 seconds. The right figure shows all nodes live at 60 seconds and all nodes that were once live but are no longer live and are identified as black squares. This is an option that can be chosen and may be useful to determine any other nodes in the vicinity of the network that may still contain some evidence of the network members or malicious behaviour even though they had closed down by the time a malicious message was sent.

The example shows what can be done if either all nodes have been successfully gathered and their evidence examined, or some isolated nodes are gathered and at least some nodes in the main network in the middle are gathered and examined. Figure 4 shows a reconstruction of the network at 10, 30 and 50 seconds and demonstrates how the reconstruction time can be entered by the forensic investigator to display the network at any given time during its lifetime. The update period for the simulation is 1 second, so at any time during the life of the network, the reconstruction can be made and is accurate to within the 1 second update period.

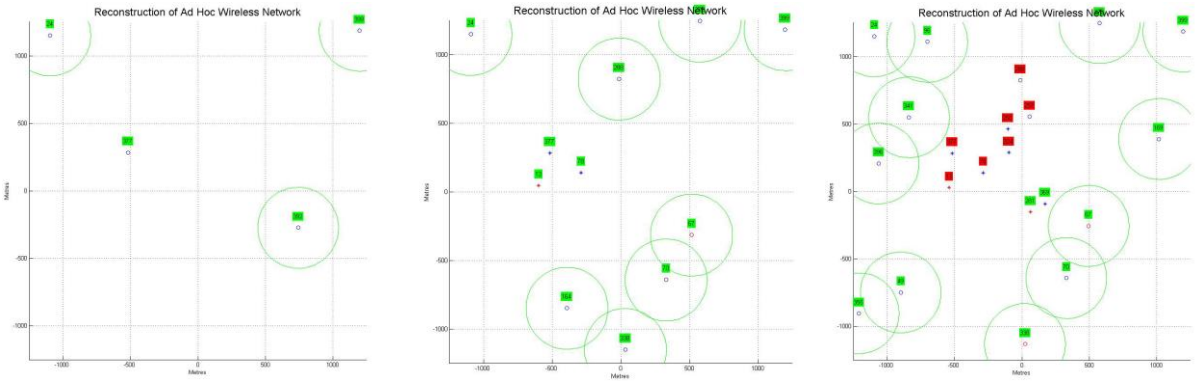

Figure 4: Reconstruction at 10, 30 and 50 seconds

Whilst the goal for the forensic investigator is to collect 100% of the devices that existed in the network, it is more likely that only a percentage of nodes can be collected and the reconstruction is therefore attempted with this limited number of nodes. Here, the amount and type of information stored in the nodes makes a significant difference in the success of the reconstruction. Figure 5 shows a similar simulation run to 60 seconds representing approximately an hour or more for the network to form. In this figure, the reconstruction is run at the 60 second mark but a limited percentage of nodes were able to be collected. Nodes that had been present in the network previously but were not live at the target time are present as black squares.

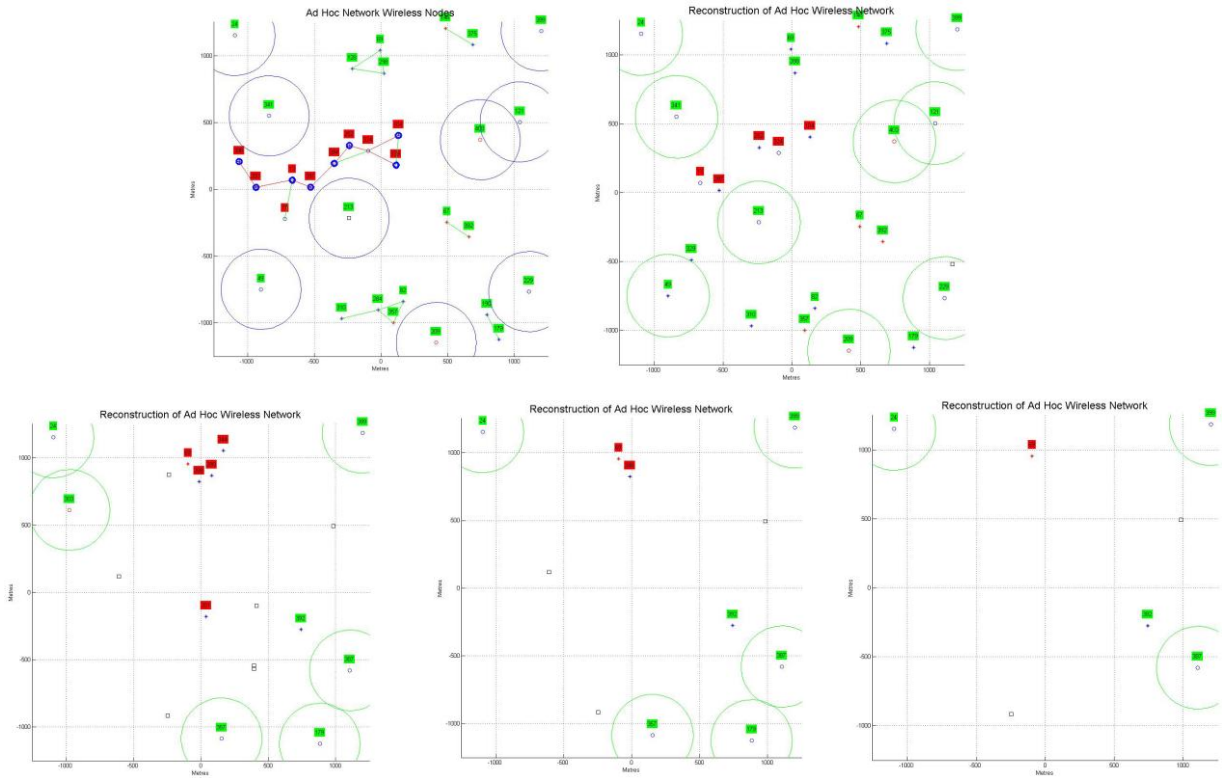

Figure 5: Network at 60 seconds, reconstruction with 80%, 50%, 30%, 20% nodes

It is apparent that relying solely on the node to be recovered to place it at the correct location in the network is problematic. Even with 80% of the total nodes recovered, there is no guarantee that this will equate to 80% of the nodes in the network of interest. If the target of the investigation is the network at centre left with 10 nodes, then the reconstruction with 80% of nodes recovered has in fact recovered only 50% of the nodes in this network although 80% are recovered overall. This is unlucky but a consequence of chance in recovering fewer than all the nodes.

Rather than rely solely on each node's information about itself, neighbouring nodes may have stored information that can be used to identify and place nodes on the grid that have not been successfully collected. This would mean that for the 5 nodes recovered from the target network, their logs which are recovered may contain sufficient information to place the remaining 5 nodes in their respective locations. If an investigation is tracing the origin of a malicious message, then the information required may be the path the message has taken which can then be traced from receiver to the nefarious sender. Acquiring the nodes utilised as hopping points for the message may not provide any more useful information, so that information about these nodes may be sufficient. This does however require that nodes collect and store the information in case a forensic investigation is undertaken later. The forensic readiness of the network could lead to a much more successful outcome by simply querying neighbours attributes on a regular basis and storing the information. At this stage of development, this has not been designed into the forensic protocol but will rather be the next stage of development for the forensic reconstruction simulation software.

CONCLUSION

Wherever a network is present, security and forensic readiness should be a major consideration. Preparing for the worst means that should some serious issue occurs that leads to the requirement for a forensic investigation of a spontaneous ad hoc network, the forensic investigator can have the best chance of the successful outcome of identifying the perpetrator by conducting a forensic investigation. It may be that serious misbehaviour in the network has led to serious injury or death with the only hope of identifying the perpetrator being the number of devices that can be recovered and the information that they contain. The development of protocols that allow for forensic readiness is something that has been largely ignored with the focus in the past more on security issues in these networks. The ability to reconstruct a spontaneous ad hoc network, possibly days or weeks after it has been disbanded is something that is urgently required by forensic investigators. The further development in this

research, it is hoped, will lead to better guidelines as to what information and what percentage of devices will likely be needed for successful forensic investigations. Further development will greatly enhance the protocol and provide results that can act as these guidelines.

REFERENCES

Cam-Winget, N., R. Housley, et al. (2003). "Security flaws in 802.11 data link protocols" Commun. ACM 46 (5): 35-39

Dewald, A. (2015). Characteristic Evidence, Counter Evidence and Reconstruction Problems in Forensic Computing. Ninth International Conference on IT Security Incident Management & IT Forensics (IMF), 2015 Megdeburg: 77-82.

Graffi, K., P. S. Mogre, et al. (2007). Detection of Colluding Misbehaving Nodes in Mobile Ad Hoc and Wireless Mesh Networks. Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE.

IEEE (1999). "IEEE Std 802.11b-1999." Retrieved 15th June 2004, 2004.

IEEE (2009). "IEEE Std 802.11n." Retrieved 8th December 2009, 2009.

Lacuesta, R., J. Lloret, et al. (2013). "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation." IEEE Transactions on Parallel and Distributed Systems 24(4): 629-641.

Kuo, W., Chu, S. "Energy Efficiency Optimization for Mobile Ads Hoc Neworks". IEEE Access, vol 4, pp928-940. doi: 10.1109/ACCESS.2016.2538269

N. Malik, J Chandramouli, et al. (2017). Using network traffic to verify mobile device forensic artifacts. Consumer Communications & Networking Conference (CCNC) Las Vegas, Nevada, USA.

Nelson, C. B., B. D. Steckler, et al. (2011). The Evolution of Hastily Formed Networks for Disaster Response: Technologies, Case Studies, and Future Trends. Global Humanitarian Technology Conference (GHTC), 2011 IEEE.

Nisbet, A. (2014). A Simulation-based Study of Server Selection Rules in MANETs Utilising Threshold Cryptography. Proceedings of the 11th Australian Information Security Management Conference, 2-4 December 2013, Perth, Australia.

Nisbet, A. and M. A. Rashid (2009). A Scalable and Tunable Encryption Key Management Scheme for Mobile Ad Hoc Networks. International Conference on Wireless Networks 2009, Las Vegas, NV.

NIST (2006). Guide to Integrating Forensic Techniques into Incident ResponseSpecial Publication 800-86.

Shimoda, K. and K. Gyoda (2011). Analysis of Ad Hoc Network Performance for Disaster Communication Models. 10th International Symposium on Autonomous Decentralized Systems (ISADS), 2011

Suzuki, H., Y. Kaneko, et al. (2006). An Ad Hoc Network in the Sky, SKYMESH, for Large-Scale Disaster Recovery. Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE 64th.

Wang, J.H., L.C. Wang, et al. (2005). Coverage and Capacity of a Wireless Mesh Network. International Conference on Wireless Networks, Communications and Mobile Computing, Taiwan, IEEE.

Zhang, Y., W. Lee, et al. (2003). "Intrusion detection techniques for mobile wireless networks." Wirel. Netw. 9(5): 545-556.