ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Challenges and Requirements of Digital Forensics Investigation in Wireless Ad-hoc Networks

Abdulrahman H. Altalhi
Department of Information Technology, College of Computing and Information Technology,King Abdulaziz University ,Jeddah, Saudi Arabia .
ahaltalhi@kau.edu.sa

Zailani Mohamed Sidek
InformationSecurity,DepartmentAdvanced Informatics School (AIS)Universiti Teknologi Malaysia 54100 Kuala Lumpur
zailani@utm.my

Labeeb Mohsin Abdullah
Electrical Engineering Faculty, Universiti Teknologi MARA, 40450
Shah Alam,Selangor, Malaysia .
labeeb96@yahoo.com

Muhammad Sufyian Mohd Azmi*
Department of Software Engineering, College of Information Technology, Universiti Tenaga Nasional,43000 Kuala Lumpur, Malaysia.
sufyian@uniten.edu.my

Abstract: Digital forensics involves the acquisition and investigation of materials that are collected from digital devices involved in digital crimes. Currently, the term "digital forensics " is used to cover the investigation of all devices used to store digital data .There are some technologies that have the ability of expanding, and wireless ad-hoc network technology is one of them. Due to the nature of wireless ad-hoc networks, difficulties commonly arise, and as a result, investigating such networks, create large challenges. Thus, the goals of this paper are to understand the concepts of wireless ad-hoc networks and the challenges of collecting live evidence on such networks, to highlight the research requirements, and to propose solutions to some of these challenges.

Keywords: Digital forensics, Wireless Ad-hoc networks, Digital crimes, Digital investigation.

I. INTRODUCTION

Network forensics plays a key role in helping investigators to take forensic decisions depending on the flow of traffic observed from a network connection to a computer, which could also be connected to an investigation course. The process of collecting a data set from a live network is difficult; thus, an approach that is different from that of storage media forensics is required. In fact, a network that has unpredictable communication channels, such as a wireless ad-hoc network, represents a major challenge for the process of forensics. Currently, different examples of ad-hoc networks exist, for instance, Wireless Mesh Networks (WMNs), Mobile Ad-hoc Networks (MANETs) and Sensor Networks Vehicular Ad-hoc Networks (VANETs).

The common characteristic among all these types of wireless ad-hoc networks is that nodes cooperate and collaborate to communicate without the need of physical network infrastructures, unlike cellular networks. Ad-hoc networks are the new example of wireless communication mobile nodes (hosts). The interesting aspect of ad-hoc networks is that they do not need a fixed infrastructure, like MSCs (mobile switching centers) or BSCs (base station centers)[1][2]. Ad-hoc network devices have the ability to operate in two ways: as clients and as routers that are able to forward packets on behalf of nodes that are not in the range of their destinations' wireless transmissions. These types of networks have the ability to be self-organized in a dynamic fashion for the purpose of automatically self-configure with the nodes in the network, also to establish and maintain mesh connectivity among themselves. These important features give many advantages to wireless ad-hoc networks, such as easier maintenance, reduction of front cost, reliable service coverage and efficiency. Classical client nodes in WMNs have the ability to be connected directly with wireless mesh routes in such a way that increasing the area of coverage by means of the mesh network backbone is possible [4]. Characteristics such as the dynamic change of membership and topology in wireless ad-hoc networks force them to use a special type of rounding protocols [5].

The use of such special types of protocols results in difficulties in performing live network forensics. Making the situation more difficult is the fact that many countries can easily set up wireless mesh networks using 802.11-based technologies without the need for a license [3]. As a result, this platform attracts many criminal activities. Therefore, it is necessary to find and use methods or (mechanisms) that have the ability to record live forensic evidence. A major goal in criminal investigation is to reconstruct the criminal scenario. This goal becomes one of the biggest challenges if we consider how complicated it is to reconstruct events or scenarios that occurred on a temporary network that can vanish without a trace and whose mobile node(s) can leave the network at any time. As a result, running live forensics in an ad-hoc network without being detected is a major challenge as well. What forensic scientists can obtain from a typical wireless ad-hoc network is the network conditions, which will provide little more than some support for forensic data collection. What researchers are seeking is a way to collect network-related data in a manner that is forensically sound.

II. AD -HOC NETWORK CONCEPTS AND APPLICATIONS

Point-to-point communication has undergone important developments via wireless technology that uses radio frequencies, microwaves, and lasers to carry data. This

technology is found, for example, in personal digital assistants mobile phones, Bluetooth-enabled computers, and household appliances such as TVs, and is used to achieve communication among devices. In fact, once a Bluetooth-enabled device becomes active, it will try to communicate with the other devices in its area to create what we call an *ad-hoc networks* or *piconet* [7]. The mobile nodes that exist in the same radio range via a wireless link will be able to communicate directly among themselves. On the other hand, those nodes that are far from the radio range will use other nodes as routers to send their messages, and as a result, the network topology for the ad-hoc network will be changed due to the changes in the frequency. Figure 1 depicts a good example of the changes in the ad-hoc network topology. The initial scenario in Figure 1 is as follows: Nodes 1 and 4 are connected by direct link. When they move out of first radio range, the link between them is broken, yet the network is still connected because 1 can reach 4 through 3, 5 and 6.

The majority of ad-hoc wireless networks applications are still within the field of military uses. For instance, planes, tanks, or soldiers that are provided with wireless communication devices will be able to form an ad-hoc wireless network when they move into a battlefield. Another application for ad-hoc networks is applicable to emergency services, law enforcement situations, and rescue operations [8]. Due to their ability to be deployed quickly and with acceptable cost, ad-hoc wireless networks are becoming a popular option for commercial uses, such as virtual classrooms and sensor networks.

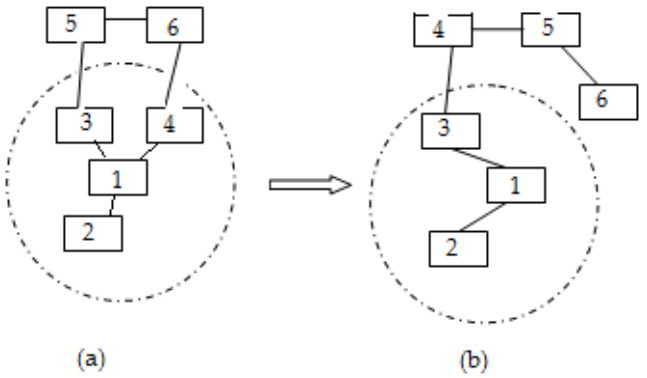

Figure 1: The change in ad-hoc networks topology that occurs in nodes 1, 2, 3, 4, 5, and 6 leads to the creation of an ad-hoc network with different topology. The radio range of node 1 is represented by the circle. The initial topology for the network is shown in (a); when node 4 changed its location outside of the radio range boundary of 1, the network topology changed to be the one in (b).

III. THE USE OF WIRELESS AD-HOC NETWORKS IN DIGITAL CRIMES

The benefits of new technology are countless, though at the same time, some disadvantages that lead to various problems also exist; wireless ad-hock network technology is no exception. To compete with criminals who use the benefits of new technology in harmful ways, law enforcement must face the great challenge of being pro-active in finding new methods to combat such crimes. Wireless ad-hoc networks present many advantages to users; however, unfortunately, numerous criminals could also take advantage of this technology. Recently, a considerable amount of research has been performed to improve the quality of service provisioning for wireless ad-hoc networks. Unfortunately, a very small amount of this research touches on other important areas, such as evidence collection. The nodes in wireless ad-hock networks are assumed to be secure, but with their unique characteristics, these nodes represent an attractive platform for suspicious activities [3]. One of the factors that influence digital crimes committed with wireless ad-hoc networks is connectivity to the Internet; some examples of such crimes will be provided to illustrate crimes in networks that are connected to the Internet and to networks that are not connected. Most of the time, stolen information from stand-alone ad-hoc networks is used to gain some type of financial benefit. The details of the user account that has been stolen in one network could be easily used to impersonate anyone. Examples of crimes that are committed in ad-hock networks, especially in the stand-alone networks are as follows:

a. Local terrorist cells that are planning or distributing information among their members for terrorist activities.
b. Illegal local sharing of copyrighted materials.
c. Tracking goods and people illegally in local areas (towns or cities) through devices associated with ad-hoc access points.
d. Illegal monitoring of people and goods in towns or cities by hacking the video surveillance system that is connected to cameras in a citywide ad-hoc network.

Seizing and stealing personal information from communications devices, such as devices that connect to a citywide ad-hoc network.

IV. DIGITAL INVESTIGATION NECESSITIES IN WIRELESS AD-HOC NETWORKS

Finding a framework for research in wireless networks and particularly in ad-hoc networks, becomes more difficult and challenging when compared with wire-line networks. Thus, a number of requirements have to be fulfilled. First, attacks are not static, but mobile, meaning that during the attack scenario, the attacker has the ability to change its point of access, position, location, and identity. Using a formal model of digital investigation in wireless networks, such mobility-based data must be combined during the modeling process action in the scenario of attack. Second, to collect mobility-based information efficiently, a number of reliable and trusted nodes must be allocated over the network and then be used to collect trusted information.

This type of nodes, known as *observers*, should be provided with a number of mechanisms and methods for the purpose of supervising; logging, tracking the events involved in node movements, topology changes, IP handoff, roaming, and creation of clusters, splitting, and merging. Third, various reactions can be conducted by the observer nodes that are distributed over the network due to events that are occurring. In scenario a), the event is probably detected and simultaneously reported by all observing nodes in the network. In b), it is detected and reported by some of the observing nodes, some of which could be out of the range of communication of both the attacker and the victim, as well as by the intermediate nodes that route the attack traffic.

The last scenario is c), in which no event can be observed because the attacker exists in a dead zone (uncovered zone). To successfully investigate the scenario of an attack, the development of correlation, filtering and

aggregation of the collected events and efficient mechanisms is necessary [9]. Fourth, to investigate an attack, secure delivery is needed to convey observations to a central investigation node. Nevertheless, as result of the effect of mobility, setting up a routing path between the central investigation and observer node is not always guaranteed. Hence, choosing the observer node in the network (depending on, for example, the availability rate of computational resources, or the degree of connectivity with other observer nodes that are responsible for traffic observation related to the attack) to control the process of collecting the observation and the attack investigation should be performed very carefully. Fifth, some malicious events included in the attack scenario, for example, targeting the network layer, result in a lack of generated evidence in the system. In contrast, some events that compromise the system cause it to have problems in recognizing and using its security software. In short, some attacks will be invisible to the network security solution. It is highly important to provide the proper mechanisms to match all types of evidence such as storage, network, and system evidence; to deal with any incompleteness in them; and to find provable system properties [9].

V. DIGITAL EVIDENCE COLLECTING AND ITS CHALLENGES IN WIRELESS AD-HOC NETWORKS

The focus of most digital investigation work is on classical wireless and wired networks. A packet sniffer is the tool usually used by forensic investigators to capture network traffic for networks that have suspicious activates. This tool (the sniffer) captures all the packets of data, even those that are aimed at other network devices or computers. Normally, copies of all packets will be sent and stored on a disk by the packet sniffer. The packet sniffer works by saving the data packet upon receiving it, and it will immediately return to listening mode to capture the next arriving packet. Sniffers have to be within the transmission range of the wireless network that is under investigation. Although using a packet sniffer in a wireless ad-hock network is possible, the unique characteristics of this type of wireless network (ad-hoc) pose many challenges, such as the following:

A. Nodes of Mobility:

In an ad-hock wireless network, nodes of mobility could be stationary or mobile. In most cases, the client nodes can be mobile. As long as the condition "Mobile nodes must be in communication range" is fulfilled, the establishment of connectivity will be ensured. The challenges in the investigation process of the mobile nodes lie in their ability to change some conditions in the network, such as topology and connectivity. This ability will add more complexity to the process of crime reconstruction for network events during the process of investigation. The number of nodes or users that participate in criminal activities may not be easy to establish; for example, if the intruders or cyber criminals use mobile nodes, it would be difficult because their location will not be easy to identify. The mobility of the node can cause nodes to disconnect, and those nodes could result in very important information being carried away from the network. Losing this information will make it nearly impossible to collect forensically sound data.

According to [11], there is a direct relation between error rate and distance in collection evidence. Distance causes a decline in the quality of the signal. Currently, the IEEE 802.11 MAC layer protocols are not efficient enough if the number of the hops is greater than three [12]. Even lower level information, such as the MAC address, is affected by the hops number between the monitored node and the investigator. If investigators were able to deploy enough devices equipped with Global Positioning System (GPS) at different points within the boundary of the network range under investigation .That using of (GPS) would be helpful for estimating the location of the nodes that are being monitored.

B. The Mechanisms of Existing Security:

Due to their unique characteristics, wireless ad-hoc networks are vulnerable to numerous security threats. Examples of such attacks include Eavesdrop attacks, Denial Of Service (DoS) attacks, and attacks aimed at routing protocols. A routing protocol is vulnerable to types of attacks such as Wormhole [11], Rushing [12], and Sybil attacks [13]. Because of the weaknesses in ad-hock networks that make them an easy target for many types of attacks, they require a great deal of work to make them more secure. Nodes are part of the mechanism used to guard against attacks. They work by sharing the security mechanism that connects to every node, such that any individual node that does not respond like other nodes will be considered to be malicious and thus will not be allowed to access the network source.

This mechanism (*Existing Security)* creates huge challenges for both researchers and the research process. If a network has been setup for the purposes of criminal activities and is run by criminals, it will be extremely difficult for investigators to collect any forensic information without being detected. In fact, the scenario that criminals and terrorists usually prefer to enact is one in which they establish a temporary network for communication in any public place, such as hotel or café, for the purposes of launching an attack. There are many mechanisms that have already been developed to solve intrusion challenges. In [14], one of the earliest mechanisms and solutions to detect intrusion was proposed. In this technique, all nodes in the networks share the process of detecting the intrusion. One of the major goals for researchers is to continue the process of developing new measures to avoid detection. These types of measures might share similarities with security attacks. For instance, advertising an incorrect sequence number could make all traffic pass through the devices of a researcher.

Nonetheless, an attack such as impersonation could lead to any nearby non-target network and might provide inaccurate evidence, which could give criminals a solid defense in a court of law if they can prove that such evidence is not precise. MAC addresses might be strong evidence, as they are unique identifiers and offer a good solution to such a problem; nevertheless, collecting such low-level information from monitored nodes poses a great challenge due to the factor of distance and its significant effects on the precision of this information. To have unquestionably solid evidence, capturing devices have to be within one hop of distance from the monitored target to collect non-routable traffic [10].

C. The Change of Network Topology:

Because of the characteristic of mobility which wireless ad-hock network have, this network can change its topology dynamically, this change in topology makes the process of recognizing network's membership more difficult. The change in the topology map, poses great challenges to the investigators in their attempts to reconstruct and find the topology state for the network under investigation at the moment the crime was committed. To solve such problems, a considerable number of topology control mechanisms have been proposed. In [14], the best topology control mechanism is proposed. The network might be divided by creating a one-way link that will make it difficult for investigators to collect data from some parts of the network. Nevertheless, taking snapshots periodically from the network and sharing these snapshots with other teams of investigators on the network may be helpful in solving the problem of topological address changes. Analyzing all the network snapshots will help to describe the crime scenario also can be very useful in reconstructing the crime scene events and scenario. To ensure the effectiveness of this technique, a mechanism to avoid detection must be employed.

D. The Unreliability of Communication Channels:

Because of its unreliable communication channels, the packet loss of wireless ad-hoc networks is usually high. This loss represents a challenge because of the high probability of losing forensic data.

E. Multi-hop communication:

One of the obstacles that forensic investigators face with wireless ad-hoc networks is that their communication is usually performed via multi-hop, making it difficult to ascertain and trace the precise origin of the network traffic under investigation. The purpose of using a wireless mesh network is to extend the coverage range of the wireless network without affecting the channel capacity [4]. To meet this goal, data packets must be forwarded by the nodes on behalf of other nodes in the event that the nodes used for communicating are not within one another's range of transmission. The potential danger of this process comes from the malicious nodes that could exist in the communication path and that are capable of modifying data packets aimed at a specific destination. Thus, it is essential to collect the suspicious origin data and determine whether the nodes that are forwarding data are contributing to the crime. From what we have observed, it is clear that obtaining such information will not be an easy task, in terms of forensically sound collection and prosecution of the perpetrators. As mentioned earlier, multi-hop communication makes it more difficult to collect accurate evidence because of the inverse relationship between distance and accuracy. Therefore, the challenge is to have as many collecting devices as possible within the monitored network because having more devices means having a greater number of chances to collect evidence; however, at the same time, the chances of being detected will increase.

F. The Challenge of low Power Devices:

At times, the network nodes are operating on battery power, causing power to become a crucial factor. Another obstacle that makes the process of forensic investigation more complex comes up when the nodes used in investigation are not driven by battery and are power constrained. In addition, the storage capacity used in investigators' devices could represent a challenge. As a partial solution, the devices used in the investigation must carefully select the data to be recorded as evidence while, at the same time, choose the most energy saving mechanism for collecting evidence. Currently, various energy efficient protocols have been presented for different layers. For instance, the work in [15] presents an energy aware routing protocol, and the work in [16] proposes an energy aware topology controller. Finally, a solar-powered device could be a good solution for overcoming the power limitation problem.

G. Inter-Operability with other Networks:

Inter-operability is a feature used by wireless mesh networks to support mesh and conventional clients. However, this feature makes it more difficult to ascertain the origin of suspicious activities on the network. Numerous types of networks, such as wireless sensor networks, have the ability to inter-operate with wireless ad-hoc networks using special nodes that are able to act as bridges; this will also lead to more complexity in the forensic process of collecting evidence.

VI. CONCLUSION

Countless advantages have arisen from the development of this technology. For instance, wireless ad-hoc networks make computer network setup easy and inexpensive. Nevertheless, some criminals take advantage of such wireless networks to plan and execute cyber attacks. The requirements and challenges of live evidence are described in this paper to illustrate methods for possible prosecution and their difficulties. The obstacles and challenges of digital forensic investigation in wireless ad-hock networks lie mainly in the unreliability of communication channels and multi-hop communication. Classical methods of forensic investigation are not sufficient to overcome all the challenges and problems, making it vital that feasible mechanisms are found to deal with wireless ad-hoc networks. We can conclude the following from this work.

First, because of the specific characteristics of wireless ad-hoc networks, collecting live evidence is not an easy job. Second, reconstructing the scene of the crime, such as the structure of the network, is one of the most complicated tasks. Finally, the use of traditional digital forensics with live networks such as wireless ad-hoc networks may not be reliable, thus making the development of new mechanisms essential. Still, there are some approaches that the investigation process can follow to improve the quality and precision of collected evidence, such as collecting more evidence by increasing the number of devices involved in the investigation process, regularly taking snapshots the network, and using GPS-enabled devices. However, the solutions proposed in this paper must be explored in greater depth. In addition, future work must propose and test solutions to the problems described in this paper.

VII. REFERENCES

[1]. M Reith, C Carr, G Gunsch (2002)."An examination of digital forensic models". International Journal of Digital Evidence. Retrieved 2 August 2010.

[2]. Various (2009). Eoghan Casey. ed. Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 0123742676. Retrieved 27 August 2010.

[3]. Murimo B. MUTANGA1, et al " Challenges of Evidence Acquisition in Wireless Ad-Hoc Networks" University of Zululand, Department of Computer Science www.IST-Africa.org/Conference2010

[4]. I. F. Akyildiz, X. W ang and W. Wang, "Wireless mesh networks: a survey," Computer Networks Volume 47, Issue 4, 15 March 2005, Pages 445-487.

[5]. M.B. Mutanga, T. C. Nyandeni, P. Mudali, S. S Xulu, M. O. Adigun, "Wise-DAD Auto-Configuration for Wireless Multi-hop Networks," In theproceedings of the Southern African Telecommunications Conference, Sept 2008.

[6]. D. Johnson, K. Matthee, D. Sokoya, L. Mboweni, A. Makan, and H. Kotze, "Building a Rural Wireless Mesh Network - A do-it-yourself guide to planning and building a Freifunk based mesh network," Wireless Africa, Meraka Institute, South Africa 30October 2007 www.wirelessafrica.meraka.org.za/wiki/images/f/fe/Building_a_Rural_Wi eless_Mesh_Network_- _A_DIY_ Guide_ v0.7_65.pdf.

[7]. Martin Olivier, Sujeet Shenoi (2006). "Advances in digital forensics II" Springer press.p. 631. ISBN 10:0-387-36890-6

[8]. Lidong Zhou et al Securing Ad Hoc Networks IEEE network, special issue on network security, November/ December, 1999.

[9]. 978-0-7695-3792-4/09 $25.00 © 2009 IEEE DOI 10.1109/SADFE.2009.16 Slim Rekhis and Noureddine Boudriga Communication Networks and Security Research Lab. University of the 7th November at Carthage, Tunisia

[10]. B. J. Nikkel, '"Improving evidence acquisition from live network sources", Digital Investigation Volume 3, Issue 2, June 2006, Pages 89-96

[11]. Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. Proactive RSA. In B. S. Kaliski Jr., editor, Advances in Cryptology—Crypto'97, the 17th Annual International Cryptology Conference, Santa Barbara, CA USA, August 17–21, 1997, Proceedings, volume 1294 of Lecture Notes in Computer Science, pages 440–454. Springer, 1997.

[12]. M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson. The digital distributed systems security architecture. In Proceedings of the 12th National Computer Security Conference, pages 305–319, Baltimore, MD USA, October 10–13, 1989. National Institute of Standards and Technology (NIST), National Computer Security Center (NCSC).

[13]. R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of RSA functions. In N. Koblitz, editor, Advances in Cryptology—Crypto'96, the 16th Annual International Cryptology Conference, Santa Barbara, CA USA, August 18–22, 1996, Proceedings, volume 1109 of Lecture Notes in Computer Science, pages 157–172. Springer, 1996.

[14]. L. Gong. Increasing availability and security of an authentication service. IEEE Journal on Selected Areas in Communications, 11(5):657–662, June 1993.

[15]. Z. J. Haas and B. Liang. Ad hoc mobility management using quorum systems. IEEE/ACM Transactions on Networking, 1999.

[16]. Z. J. Haas and M. Perlman. "The performance of query control schemes zone routing protocol". InSIGCOMM'98, June 1998.

