IST-Africa

IST-Africa 2010 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2010
ISBN: 978-1-905824-15-1

Challenges of Evidence Acquisition in Wireless Ad-Hoc Networks

Murimo B. MUTANGA[1], Pragasen MUDALI[1], Innocentia Z. DLAMINI[2], Lonias NDLOVU[3], Sibusiso S. XULU[1], Matthew O. ADIGUN[1]
[1]*University of Zululand, Department of Computer Science*
KwaDlangezwa, 3886, South Africa Tel: +27359026706, Fax: + 27359026750, Email: bethelmutanga@gmail.com
[2]*Department of Defence, Peace, Safety and Security, CSIR, Pretoria, 0001, South Africa Tel: +2712 841 3224, Email: idlamini@csir.co.za*
[3]*University of Zululand, Department of Mercantile Law*
KwaDlangezwa, 3886, RSA, Tel: +27 35 90262136, Email: lndlovu@pan.uzulu.ac.za

Abstract: Network forensics plays a major role in the investigation of criminal activities involving computer networks. Investigating such crimes is still an open research area due to the fact that technology is always advancing hence investigators must always be up-to-date with technological advancements. Wireless ad-hoc networks are one of the technologies that have the potential to expand. Due to the unpredictable nature of wireless ad-hoc networks, carrying out investigations in these networks poses a big challenge. Thus, the aim of this paper is to explore the challenges of acquiring live evidence in wireless ad-hoc networks. We also give some legal requirements of evidence admissibility as outlined in the Communications and Transactions Act of South Africa. An analysis of these challenges will help investigators to come up with effective measures for live evidence acquisition in wireless ad-hoc networks. We also highlight possible solutions to some of the challenges identified in this paper.

Keywords: Digital forensics, wireless ad-hoc networks, Network forensics, Evidence.

1. Introduction

Network forensics makes it possible for investigators to make forensic determinations based on the observed traffic on a computer network, which may be relevant in the course of an investigation. The difficulties in collecting a complete set of data from live network sources require an approach different from traditional storage media forensics. This is a huge challenge if the network has unpredictable communication channels like wireless ad-hoc networks. Today we can find several instances of ad-hoc networks: Mobile Ad-hoc Networks (MANETs), sensor networks Vehicular Ad-hoc Networks (VANETs), Wireless and Mesh Networks (WMNs). In all these types of wireless ad-hoc networks, nodes collaborate to allow communication without the required presence of a physical network infrastructure such as in cellular networks. Network devices operate not only as clients but also as routers, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. These networks are dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves. These features brings many advantages

to wireless ad-hoc networks such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. Conventional client nodes in WMNs can connect directly to wireless mesh routers thereby increasing the coverage area of the wireless mesh network backbone [1]. Due to their dynamically changing membership and topology, wireless ad-hoc networks use specialized routing protocols [2]. This complexity makes it difficult to perform live network forensics. In most countries, ad-hoc networks such as, wireless mesh networks can be setup without a license by using 802.11-based technologies [3]. This makes it an attractive platform for criminal activities. Crime syndicates all over the world use computer networks to conduct their operations [4]. It is therefore imperative to come up with mechanisms that can record live forensic evidence in such an environment.

One major goal of criminal investigation is to reconstruct the criminal events or the scene of the crime. This task becomes challenging when one considers how difficult it is to re-construct events that take place on a temporary network that can disappear without a trace and having mobile nodes that can leave the network at any time. Performing live forensics in such a network without being detected is also a big challenge. A typical wireless ad-hoc network presents forensics scientists with network conditions that provide little support for forensic data collection. Investigators seek to collect network-related data in such a way that it may be forensically sound. When forensic soundness includes the ability to stand up to legal scrutiny in a court of law, the effort involved can be extremely expensive in terms of labour and time, and even at that, the effort may not be successful. A major reason legal remedies are not pursued in cyber intrusion cases, is the cost and level of effort required for reactive investigations [5]. It is therefore imperative that as much suspicious traffic as possible be captured and this must be done proactively.

Computer forensic investigation is normally a four step process, namely acquisition, identification, evaluation and presentation of evidence. This paper focuses on the acquisition aspect. There are basically two scenarios for acquiring evidence on a computer network: the incident has already occurred or the incident is currently in progress. Our interest is on the latter in an ad-hoc network scenario. If the incident is ongoing, the investigator has to capture the activities in real-time. Tools such as snifers or monitors can be used to collect evidence as it unfolds [4].

Traditional digital forensics mechanisms attempt to preserve all evidence in an unchanging state, while live digital forensic techniques seek to take a snapshot of the state of the computer, similar to a photograph of the scene of the crime hence the interest. Infact the need for conducting forensic analysis of live systems has escalated over the years [6]. Criminal and malicious users continuously devise new methods and places to hide their activities [7]. Performing live forensic investigations has, thus, become a trend in digital forensics and numerous vendors are implementing their own investigation procedures. Traditional digital forensics techniques and procedures cannot be employed on live networks because in most cases it requires one to switch off the network devices and carry out the investigation. However, information about what is happening on a running network can be lost when the network or the computers that are involved are switched off. Actually forensic data gathered from a live system or network can provide evidence that is not available in a static disk image [6]. It is however, important to note that live forensics operates with unique and challenging constraints. Specifically, the evidence gathered represents a snapshot of a dynamic system that cannot be reproduced at a later date [6]. This can be more complicated if one considers challenges posed by wireless networks such as wireless ad-hoc networks.

This paper explores the challenges of collecting evidence in wireless ad-hoc network. In this paper we have deliberately omitted the legal aspects of obtaining the network capture rights because there are various jurisdictional rules with regard to obtaining lawful

intercepts of network communications, which fall outside the scope of this work. We however included legal factors affecting the admissibility and weighing of evidence in South African courts of law. The rest of the paper is organised as follows. In section II we present some scenarios where ad-hoc networks can be used for criminal activities while section III briefly discusses legal issues on evidence admissibility based on the Communications and Transactions Act of 2002 of South Africa. Section IV then gives challenges of live network forensics in wireless ad-hoc networking environment. Finally section V concludes this paper.

2. Wireless Ad-Hoc Networks as a Potential Platform for Digital Crimes

Whilst new technologies bring many benefits, they also pose various problems. Law enforcers need to be pro-active in learning new ways of combating crime that comes as a result of the latest technologies and it is thus imperative to explore these challenges. Wireless ad-hoc networks have the potential to bring about numerous advantages to consumers but unfortunately criminal elements may also take advantage of such networks. In recent years, a significant amount of research in wireless ad-hoc networks has concentrated on improving Quality of Service provisioning. Unfortunately, the same intensity has not been applied to other important related areas, such as evidence acquisition. In wireless ad-hoc networks, nodes are assumed to be trustworthy, but this may not be the case as their unique characteristics makes them an attractive platform for criminal activities.

Connectivity to the Internet influences the types of digital crimes that can be committed using wireless ad-hoc networks and we thus provide examples of such crimes in networks that are connected to the Internet as well as those networks that are not. Information stolen from stand-alone ad-hoc networks can often be used in similar networks that have access to the Internet in order to achieve financial gain. User account details stolen in one network can be used to impersonate someone, amongst committing other crimes in an ad-hoc network that has Internet access. Examples of such crimes on stand-alone networks include:

- Local terrorist cell – sharing of information and planning of terrorist activities.
- Illegal, localised sharing of copyright material
- Illegal tracking of goods and people within towns and cities – via the association of devices with ad-hoc access points
- Illegal surveillance of goods and people within towns and cities – hacking into video surveillance that is obtained from cameras connected to a city-wide ad-hoc network
- Stealing of personal information from PDA's and other communication devices – these devices connect to a city-wide ad-hoc network and can be hacked into to obtain personal information.

The Internet is a major source of computer crime and wireless networks are proving to be a cheaper way for internet connectivity. Ad-hoc networks can easily be used to connect a number of people to the internet with minimal setup costs and efforts. This makes ad-hoc networks a possible launch area for criminal attacks. The scenarios below are some of the examples of criminal activities that can be launched on the internet via ad-hoc networks.

- Illegal, internationalised sharing of copyright material
- Botnets that spread malware - and collect infected user information such as user accounts, contact lists, etc.
- Sources of Denial of Service (DoS) attacks
- Sources of 419 scams: criminals might take advantage of the temporary nature of these networks and use them to send emails and messages intended at obtaining money illegally.

- Sources of credit card fraud - where fraudulent purchases are made from these networks

3. Admissibility of Digitally Collected Evidence in South African Courts of Law

For evidence to be accepted in a court of law certain procedures have to be followed and the evidence must be forensically sound. Generally the nature of computer and electronic evidence poses special challenges for its admissibility in court proceedings hence security policies and mechanisms must address these challenges [4]. As an example, Section (15) of the Electronic Communications and Transactions Act of 2002 [8] of South Africa specifies the following with regards to network traffic evidence.

i. In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message in evidence:
   - On the mere grounds that it is constituted by a data message; or
   - If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

ii. Information in the form of a data message must be given due evidential weight

iii. In assessing the evidential weight of a data message, regard must be had to:
   - The reliability of the manner in which the data message was generated, stored or communicated.
   - The reliability of the manner in which the integrity of the data message was maintained.
   - The manner in which its originator was identified

The electronic communications Act allows data messages to be treated as legally accepted instruments in many aspects of the law including the law of evidence. One cannot reject evidence because it is in the form of a data message. The fact that the evidence is a data message cannot be the basis of denying its admission. It is clear that the admissibility of evidence is not an issue but the weighing of the evidence is much stricter. For example, the intruder or perpetrator of a digital incident responsible for the initial development and dissemination of the data message has to be identifiable or identified with reasonable certainty. This requirement might be difficult to meet because of routing attacks such as impersonation. It is difficult to prove the originality of a data message beyond reasonable doubt hence difficult to convincingly identify suspects.

4. Challenges of Evidence Collection in Wireless Ad-hoc Networks

Most work on evidence acquisition focuses on wired and conventional wireless networks. Forensic investigators usually use packet sniffers to capture suspicious network traffic. Sniffers capture all the data packets including those that are destined for other network devices or computers. Basically packet sniffer duplicates all packets and stores them to disk. A packet sniffer must capture and then save a data packet and return to listening mode before the next packet arrives. In a wireless network, sniffers need to be within the transmission range of the nodes or devices being investigated. Although it is possible to make use of packet sniffers in wireless adhoc networks, their unique characteristics may pose challenges such as the challenges listed below.

a) Mobility

Nodes in a wireless ad-hoc network can either be mobile or stationary. In most instances client nodes can be mobile. As long as the mobile nodes are within the communication range of the network, connectivity can always be established. Mobile nodes pose a challenge in the investigation process because they change network conditions like

connectivity and topology. This makes it difficult for cyber investigators to reconstruct the network (criminal) events during investigation. The number of nodes or users involved in criminal activities would be difficult to establish. If the intruders use mobile nodes, their location would also be difficult to establish. Node mobility can disconnect some nodes with vital information from the network, making it impossible to extract forensically sound data. According to [9], the effect of distance on the collection of evidence can have an impact on the error rate. The distance in such networks will cause a decrease in the signal quality. At present, the IEEE 802.11 MAC layer protocols cannot achieve a good throughput as the number of hops increases to more than three [1]. The ability to collect lower level information, such as a MAC address is also affected by the number of hops between the investigator and the node under investigation.

Investigators can deploy devices at various points within the range of the network being investigated. If the devices used by investigators are equipped with Global Position Satellite (GPS) system, a rough estimation of the location of suspicious devices may be established. An analysis of GPS coordinates and routing tables can help estimate the relative position of suspicious nodes.

b) Existing Security Mechanisms

Because of their unique characteristics, there are various security threats to wireless ad-hoc networks. Examples of such attacks include denial of service (DoS), impersonation, eavesdropping and attacks against routing protocols. Routing protocol attacks include wormhole attacks [10], Rushing attacks [11] and Sybil attacks [12]. Because of these vulnerabilities, a lot of work has been done in trying to make wireless ad-hoc networks more secure. Nodes collaborate to protect against these attacks. This is normally achieved by sharing a common security mechanism that is distributed on all the nodes. Any node that does not comply with the rest of the network will be regarded as malicious hence will be denied access to network resource. This poses a great challenge to the investigators. If the network has been setup solely for criminal activities, hence run by criminals, it would be difficult for investigators to collect forensic data without detection. A typical scenario could be a temporary network run by terrorist for communication in a hotel or public place before launching an attack. So many intrusion detection mechanisms have been developed. In [13] one of the first intrusion detection mechanisms was proposed. In this mechanism, every node in the network participates in the detection of intruders. Other proposals have since emanated and are continuously being refined in-order to address security issues in wireless ad-hoc networks. Investigators must continuously develop new measures to avoid detection. These measures could be similar to security attacks, for example, advertising wrong sequence numbers so that all the traffic will pass through the investigator's device.

Security attacks like impersonation might implicate the wrong person thereby providing false evidence. This attack makes it difficult to fulfil the requirements of section (iii) of the Communications and Transactions ACT [8] that deals with the manner in which the actual origin of the data in question is identified. Criminals might also use it as a defence in a court of law. If it can be demonstrated that impersonation is possible then the admissibility of such evidence will be questionable. Unique identifiers such as MAC addresses can be the best solution to this problem but the ability to collect such low level information from suspicious nodes is also greatly affected by distance. Actually, capturing devices only need to be one hop away from the target to collect non-routable traffic [9]. Even if it was possible to capture MAC addresses for nodes that are more than one hop away, MAC address spoofing still remains a hindering factor.

c) Network Topology Changes

Due to mobility and related issues, wireless ad-hoc networks have dynamically changing topologies making it difficult to determine the membership of the network. This presents investigators with a challenge when trying to reconstruct or determine the state of the network at the time of the crime. The effect of topology control algorithms on evidence acquisition also pose a potential challenge since they change network conditions that could otherwise have been favourable for investigators. So many topology control mechanisms have been proposed. In [14], a token based topology control was proposed. In this mechanism, the network may be partitioned by the creation of unidirectional links hence making it difficult for investigators to acquire network data from some parts of the network. Taking periodic snapshots of the network and sharing them with other investigators on the network could help address topology change issues. An analysis of all the network snapshots will aid in the reconstruction of the crime scene events. Mechanisms of avoiding detection must be employed if this approach is to be effective.

d) Unreliable Communication channels

Due to unreliable communication channels in wireless ad-hoc networks, packet loss is usually high. This poses a challenge since vital and incriminating forensic data may be lost as well.

e) Multi-hop Communication

Communication in wireless ad-hoc networks is usually multi-hop, making it difficult to trace the exact origin of suspicious network traffic. For example one reason to use Wireless Mesh networks is to extend the coverage range of current wireless networks without sacrificing the channel capacity [1]. To meet this and other objectives, nodes forward data packets on behalf of other nodes if the communicating nodes are not within the transmission range of each other. Malicious nodes along the communication path may modify data packets intended for specific destinations. It is imperative then to establish the exact origin of suspicious data. It is also important to establish whether the nodes forwarding suspicious data are accomplices of the criminals or not. All this information is difficult to establish yet it makes the collected data forensically sound and complete to prosecute the perpetrators. Multi-hop communication may also increase the distance between the investigator and the source of the crime. Distance impacts negatively on the data error rate hence the investigator might not get accurate or complete evidence data to prosecute the perpetrators. The biggest challenge therefore is to have as many evidence collecting devices as possible within the network. More devices enhance the chances of gathering more evidence but might however increase the chances of being detected.

f) Low Power Devices

In some instances, the network nodes are battery driven which will make the power budget a crucial factor. This becomes more complex if the node used for investigation is also power constrained. The storage capacity of the investigator's device might also pose a challenge. The investigating device must consciously select the data to record as evidence. Energy efficient mechanisms for evidence collection are therefore of paramount importance. Many energy efficient protocols have been proposed for different layers. For example the work in [15] proposes an energy aware routing protocol whilst [16] proposes an energy aware topology control scheme. How such proposals can be exploited to save energy during evidence acquisition is an area that needs to be explored. Use of solar powered devices could also help avert power limitations.

g) Inter-Operability with Other Networks

Generally, inter-operability is a desired feature in wireless mesh networks hence it can support both conventional and mesh clients. This feature makes it difficult to ascertain the origin of criminal activities on a network. Various types of networks, including wireless sensor networks and other types of networks can inter-operate with wireless ad-hoc networks using specialised nodes that can act as bridges.

5. Conclusions

Technological advancements bring about numerous advantages to consumers. In particular, wireless ad-hoc networks provide an easy and cheaper way to setup a computer network. However, criminal elements may take advantage of such technologies to plan and execute electronic attacks. For possible prosecution to occur, we investigated the requirements for the admissibility of electronic evidence in a South African court. In addition, this paper also reviews possible challenges in acquiring live evidence in wireless ad-hoc networks. Mobility, multi-hop communication and unreliable communication channels are some of the challenges that make the process of evidence acquisition in wireless ad-hoc networks difficult. Traditional methods usually require one to switch off the computer system, but in live network forensics vital information might be lost. It is therefore imperative to come up with mechanisms that make digital forensics feasible in wireless ad-hoc networks. Providing solutions to these challenges will help investigators to come up with measures for live evidence acquisition in wireless ad-hoc networks.

There are several conclusions that one can draw from this work. (1) The acquisition of evidence in live wireless ad-hoc networks is not an easy task due to the characteristics of these networks, (2) reconstructing the crime scene (the network structure and conditions) of a network that may have been dismantled is a challenging task, (3) traditional digital forensics may not be applicable to live network forensics specifically to wireless ad-hoc networks. We identified some evidence acquisition approaches that investigator can take: Increasing the number of devises that collect evidence, taking regular snapshot of the network, using GPS enabled devices, etc. However these approaches need to be explored further. The future focus of this work will be aimed at providing and testing solutions to the problems outlined in this paper.

References

[1] 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

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

[3] 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 ,” http Wireless Africa, Meraka Institute, South Africa 30 October 2007 www.wirelessafrica.meraka.org.za/wiki/images/f/fe/Building_a_Rural_Wireless_Mesh_Network_-_A_DIY_Guide_v0.7_65.pdf

[4] R. Newman, “Computer Forensics - Evidence Collection and Management”, Auerbach Publications; (9 Mar 2007) ISBN-10: 0849305616

[5] B. Endicott-Popovsky D. A. Frincke and C. A. Taylor, “A Theoretical Framework for Organizational Network Forensic Readiness”, Journal of Computers, VOL. 2, NO. 3, MAY 2007

[6] F. Adelstein, “Live Forensics: Diagnosing Your System Without Killing It First”, Communications of the ACM, Vol. 49, No. 2, February 2006

[7] B. J. Nikkel, “An introduction to investigating IPv6 networks,” Digital Investigation Volume 4, Issue 2, June 2007, Pages 59-67

[8] Electronic Communications and Transactions Act, Number 25 of 2002, (South Africa)

[9] B. J. Nikkel, '"Improving evidence acquisition from live network sources", Digital Investigation Volume 3, Issue 2, June 2006, Pages 89-96
[10] Y. Hu, A. Perrig and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad-hoc Networks," in Proceedings of IEEE INFOCOM'03, 2003.
[11] Y. Hu, A. Perrig and D. Johnson, "Rushing Attacks and Defense in Wireless Ad-hoc Network Routing Protocols," in Proceedings of ACM MobiCom Workshop - WiSe'03,2003.
[12] J. R. Douceur, The Sybil Attack, in Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), pages 251–260, March 2002, LNCS 2429.
[13] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pages 275–283, Boston, Massachusetts, August 2000.
[14] P. Mudali, "The effect of topology control for Wireless Multi-hop Networks", Masters Thesis, University of Zululand 2008
[15] Z. Wu, H. Song, S. Jiang and X. Xu, "Energy-Aware Grid Multipath Routing Protocol in MANET", Proceedings of the First Asia International Conference on Modelling & Simulation, Pages 36-41 2007
[16] A. Konstantinidis, K. Yang , H. Chen and Q. Zhang, "Energy-aware topology control for wireless sensor networks using memetic algorithm" Computer Communications Volume 30, Issues 14-15, 15 October 2007, Pages 2753-2764