International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 2 Issue 2 February 2016

An Investigation of Similar Factor of Intention of Attacks in Wireless Network

Mr. Bhupendra Sharma [1], Mr. Vikrant Sharma [2]

M-tech scholar VITM Indore [1], Asst. Prof. VITM Indore[2]
bhuppisharma2012@gmail.com[1], vikrant.s@vitmindore.com[2]

ABSTRACT:- As the expansion of technology and promotion of application, mobile devices are repetitively becoming useful in people's daily lives. Mobile devices are an evolving form of computing, used widely for personal and organizational purposes. These compact devices are useful in managing information, such as contact details and appointments, and corresponding electronically but at the same time, they are also becoming more creditable of attention as a new tool of crime, such as the use of mobile phones in the fraud, selling fake products, spreading rumors, and other illegal and criminal activities. Therefore, the judicial authorities need to invent mobile forensic to deal with the phone criminal cases or with illegal activities. Network forensic is the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities". The ultimate goal of the network forensics is to provide sufficient evidence to prosecute the perpetrator of the crime. In network forensics, finding intentions of attacker is very difficult task. To sort out this problem, earlier researchers suggest algorithm to find intentions of attack happened on network. But this algorithm is not able to find similarity intention of new attack with intention of existing attack. The goal of the work is to find close similarity between new attack intentions and existing attack intentions as well as to predict future attack on the basis of the similarity between attack intentions.

KEYWORDS:- ***Wireless Network, Forensic, cyber crime, SIA, NIA, PyFlag***

1. INTRODUCTION

The world is increasingly dependent on digital sources of information and the computerized systems and networks involved in data storage, processing, and transmission. This growing dependence drives development to advance required technology. This maturity results in technologies that will allow for data volumes unique. The offenders, criminals, terrorists, and other despicable members of society have not overlooked these facts. So words like cybercrime, cyber-war, and cyber-terror have started to become more commonplace, and organizations are being formed to stop the activity digital forensic terms define [1]. Digital forensics is a discipline of forensic science deals with the use of digital information as source of evidence in investigations and legal activities. Digital forensic is the process of perpetuation, compilation, recognition, analysis, documentation and presentation of digital evidence derived from digital sources. Digital forensic investigation process divided in four stages: collection, preservation, examination and analysis.

1.1 Computer Forensic

Computer forensics determines evidence that particular computers have been used in the conducting of crimes. Computer forensics can be defined to the forensic examination of computer components and their data. These computer components can be printers and storage media such as hard drives or CDs. In general, computer forensics is used to identify evidence when personal computers are used in the commission of crimes.

1.2 Network Forensic

Network forensic is the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities". The ultimate goal of the network forensics is to provide sufficient evidence to prosecute the perpetrator of the crime [3].

2. RELATED STUDY

M. Rasmi, Aman Jantan et al. [4] addressed the classification process and clustering of network events may arise when the protocols exist. The problem may be important to supports investigators in bringing close criminal cases with greater accuracy in advance to decide the suitable incident response. Additionally, analyzing attack intentions is a necessity to produce clear evidence to accelerate the decision processes required for apprehending the real perpetrator.

M.I. Cohen et al. [5] discussed PyFlag is a general purpose, open source, forensic package which merges disk forensics, memory forensics and network forensics. It also described PyFlag architecture and in particular how that is used in the network forensics context. The novel processing of HTML pages is described and the PyFlag page rendering is demonstrated. PyFlag's novel processing of complex web applications such as Gmail and other web applications is described. Finally PyFlag's report generation capabilities are demonstrated. PyFlag is emerging as a capable platform for network forensic analysis featuring advanced reconstruction of web pages.

R.C. Joshi et al. [6] discussed the analysis phase in network forensics approaches faces many challenges such as reconstruction methods of attack behaviour. Normally we have to go through a full capture of malicious behaviour in order to understand the intention of the attack. Also, the classification process and clustering of network events as mentioned, may arise when the protocols' complexity exist. Furthermore, reconstruction methods, which are used to understand the intention of the attack, complicate the cyber-crime analysis.

Peng et al. [7], attack intentions are realized when it is able to identify the goal of this attack, which presents its path. However, a graph algorithm with methods for intrusive intention recognition used to analyze the attack path in advance to discover the goal of the cyber crimes

Geoffrey M. Voelker et al. [8] presented a methodology for measuring the conversion rate of spam. Using a parasitic infiltration of an existing botnet's infrastructure, and analyzed two spam campaigns: one designed to propagate a malware Trojan, the other marketing on-line pharmaceuticals.

3. PROPOSED APPROACH

The goal of the work is to proposed approach to find close similarity between new attack intentions and existing attack intentions as well as to predict future attack type on the basis of the similarity between attack intentions. The proposed approach is aware to network resources from different kind of attacks in future. Proposed approach use AIA algorithm to find intentions of attack and maintain list which contain different probability values for intentions of different attacks types. The proposed approach works in following steps.

Step-1: Create N number of attack which has different intentions in network simulator considering n number of nodes and m number of attackers. Suppose value of N defined by 3 means 3 attacks is created with different intentions. First attack has intention is to degrade lifetime of network through flooding. Second attack has intention to degrade performance of network via dropping. Third attack has intention is to misguide source to select wrong route.

Step-2: After creating attacks, intentions of attackers are determined by applying Similarity of Attack Intention (SIA) algorithm that is based on Attack Intention Analysis (AIA) Algorithm. Probability value is assigns to each determined intention and represented in tabular form.

Step-3: New attack is created and its intention is determined in probability value. New attack may have similar intention of existing which given in table.

Step-4: Now intention of new attack is compared with existing intentions of attacks. Then attack has similar intention of existing attack.

Step-5: If intention of new attacks is similar then existing one then there chance of attack has similar intentions occurred in future.

4. SIMULATION

Proposed approach is simulated in Network Simulator-2(NS-2) tool considering different network simulation parameters that shown in table.

Table I. Network Parameters and Values

Parameters Name	Value
Number of nodes	10
Dimension of simulated area	800×600
Simulation time (seconds)	45
Radio range	300m
Traffic type	CBR, 3pkts/s

Packet size (bytes)	512
Routing Protocol	AODV
Connection Type	TCP

4.1 Simulation Scenario

Proposed work is simulated creating several attack scenarios considering table 1 parameters. One among them shown below figure 1

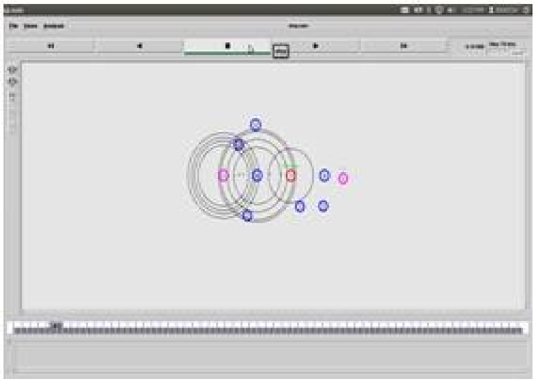

Fig: 1 Simulation Scenarios

4.2 Evaluation Parameters

The network performance is evaluated by considering following network attack scenario and its key parameters.Packet Delivery Ratio- Packet delivery ratio (PDR) obtained by received packet divided by sent from the trace or data file.

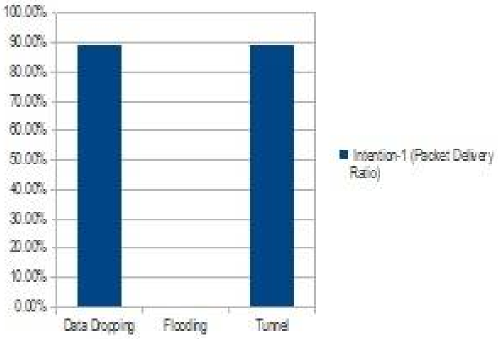

Fig: 2 Packet Delivery Ratio Graph

Throughput- Data units received in form of bits, bytes or packets per unit time are known as throughput.

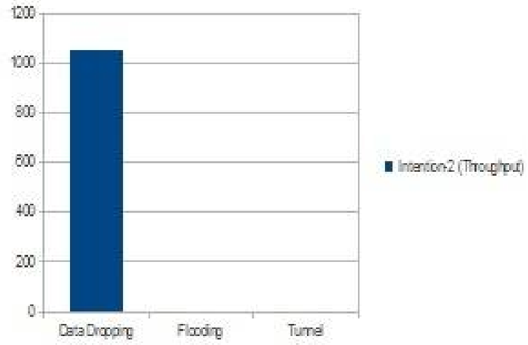

Fig:3 Throughput Graph

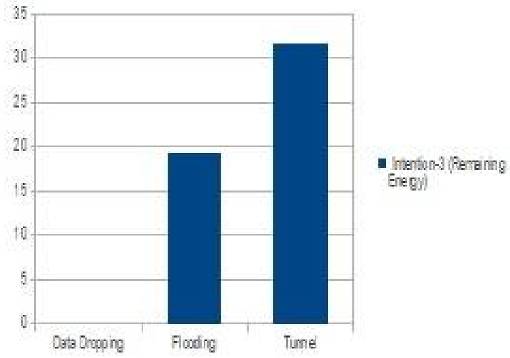

Fig: 4 Remaining Energy Graph

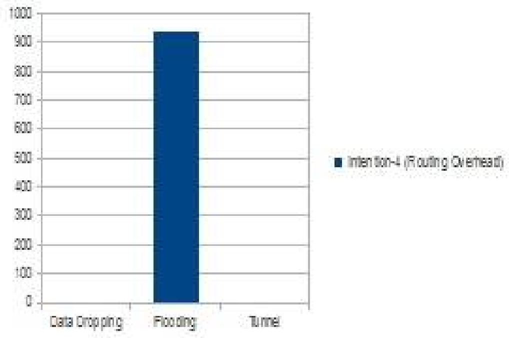

Fig: 5 Routing Overhand Graph

5. CONCLUSION

Network forensic is the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyse, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities”. The ultimate goal of the network forensics is to provide sufficient evidence to prosecute the perpetrator of the crime. In network forensics, finding intentions of attacker is very difficult task. To sort out this problem, earlier researchers suggest algorithm to find intentions of attack happened on network. But this algorithm is not able to find similarity intention of new attack with intention of existing attack. This work found close similarity between new attack intentions and existing attack intentions as well as to predict future attack on the basis of the similarity between attack intentions. Proposed work is simulated in NS-2 and evaluated considering some parameters.

REFERENCES

[1]. “A Road Map for Digital Forensic Research Report” From the First Digital Forensic Research Workshop (DFRWS)

[2]. Palmer, G., A Road Map for Digital Forensic Research, in Report from DFRWS, F.D.F.R. Workshop, Editor.: Utica, New York. 2001: p. 27–30.

[3]. Shin, Y.-D., New Model for Cyber Crime Investigation Procedure. JNIT: Journal ofNext Generation Information Technology, 2011. 2(2): p.1-7.

[4]. Mohammad Rasmi, Aman Jantan,” A New Algorithm to Estimate the Similarity between the Intentions of the Cyber Crimes for Network Forensics”, The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)

[5]. Cohen MI. PyFlag: an advanced network forensic framework. In: Proceedings of the 2008 Digital Forensics Research Workshop. DFRWS, http://www.pyflag.net; August 2008 [accessed 06.03.09].

[6]. Pilli, E.S., R.C. Joshi, and R. Niyogi, Network forensic frameworks: Survey and research challenges. Digital Investigation, 2010. 7(1-2): p.14-27.

[7]. Peng, W., S. Yao, and J. Chen. Recognizing Intrusive Intention and Assessing Threat Based on Attack Path Analysis. in Multimedia Information Networking and Security, 2009. MINES '09. International Conference on. 2009.

[8]. Kanich Chris, Kreibich Christian, Levchenko Kirill, Enright Brandon, Voelker Geoffrey M, Paxson Vern, Savage Stefan. Spamalytics: an empirical analysis of spam marketing conversion. Commun ACM 2009;52(9). ISSN: 0001- 0782:99e107.