Reliability Theory Application of Bipolar Network in Monitoring and Detecting Network Intrusion

Doan Thanh Binh [1,*], Nguyen Trung Hien[2], Do Manh Ha[3], Dinh Thi Nhung[4]

[1] *Electric Power University, No.235 Hoang Quoc Viet, Bac Tu Liem, Hanoi, Viet Nam*

[2] *BacNinh Telecommunications, No. 33, Ly Thai To, Suoi Hoa, Bacninh, Viet Nam*

[3] *ThuongMai University, No. 79, Ho Tung Mau, Cau Giay, Hanoi, Viet Nam*

[4] *Hanoi University of Science and Technology, No. 1, Dai Co Viet, Hai Ba Trung, Hanoi, Viet Nam*

Received: September 03, 2019; Accepted: November 28, 2019

Abstract

Today the rapid and widespread development of computer networks and computer network environments brings many risks and threats to network security that cause loss or change data of information systems. Security attacks that change the state and components of the system will leave traces, so tracing for network security attacks is of interest. Depending on the monitoring environment and the protocols used to transmit information between network nodes, tracking of network security attacks is done in different ways. Network security attacks affect the communication of information between network nodes, changing the dynamic relationship between network nodes and their reliability. The problem of evaluating internal network reliability to trace network intrusion detection is given and resolved in this article

Keywords: Bipolar network, detecting network, theory application

1. Introduction

Tracing is a security mechanism that helps network security personnel detect the cause, detect network intrusion. There are basically three main trace methods: (i)Trace techniques are proposed at operating system level and network level [1], [2], this technique uses network structure and communication protocols to trace network intrusion; (ii)Trace techniques are proposed at storage level [3], this technique uses a change in stored data, allowing server to track this change to detect illegal intrusion; (iii)Intrusion tolerance technique [4], [5], this technique separates anti-intrusion process from application processing, which is done through middleware-based solutions.

Operational-level and network-level trace techniques allows identification of a set of information to help identify intrusion machines and relate to level where trace technique is implemented, but at level of managing additional information regarding operational processes can be used to trace attacks. At executive level, an investigator needs to capture and analyze system activities to identify harmful entities, harmful methods and harmful effects of systems. Evidence of operating-level attacks is usually log files (a collection of active service and application information). This method only allows investigating events related to processing applications with selected administrator attributes, unable to handle attack actions to change the operations of processes. It is not possible to track attacks that implement encryption or attack mechanisms in the form of insertion and elusive [2], [6]. The methods have been proposed in [1] to overcome these drawbacks by basing on logs at kernel level of operating system. These logs help to trace the source of intrusions that are independent with applications on it.

A mobile ad hoc network can be modeled by undirected graph *G(V(t), E(t))* that change over time, where *V(t)* and *E(t)* are respectively are combinations of nodes and connections in data network at *t* time. Each node has an operating probability of p_n. Our issue is to calculate the probability of an active path between source node n_s and destination node n_d, this probability is represented by $Rel_{n_s,n_d}(G)$. In all nodes, only source and destination nodes are allowed to move freely according to a mobile model. Therefore, bipolar reliability is a function of time and frequently changes with node movements, node errors and boundary errors (edges)

Each boundary $e \in E$ has a probability of operating p_e depending on operating probabilities of nodes and connecting edges. Therefore, p_e of boudary e is connecting with node n_i and n_j can be represented by $p_e = P_r$ (e exists| n_i and n_j are active). Then each edge *e* can have one or two operating states or errors,

* Corresponding author: Tel.: (+84) 904454355
Email: Binhdt@epu.edu.v

which can represent state of network with a vector $S(t) = [S_1(t), S_2(t), \ldots, S_e(t)]$. The e-element of $S(t)$ equals to 1 if the boundary e is active and otherwise is 0. Therefore, probability of state $S(t)$ will be as follows

$$P_r(S(t)) = \prod_{e=1}^{E} p_e^{S_e(t)} (1 - p_e)^{1-S_e(t)} \quad (1)$$

We use function ψ_{n_s,n_d} to investigate states. This function checks if there exists at least one path between n_s and n_d. If state $S(t)$ consists of one or more paths between two nodes, then $\psi_{n_s,n_d}(S(t)) = 1$, otherwise $\psi_{n_s,n_d}(S(t)) = 0$. Therefore, bipolar reliability is determined as follows:

$$Rel_{n_s,n_d}(G(t)) = \sum_{allS(t)} \psi_{n_s,n_d}(S(t)) P_r(S(t)) \quad (2)$$

The structure of this article is as follows: In Part 2 we evaluate bipolar reliability in a mobile environment. In Part 3, we present method of detection and trace techniques at system level

2. Evaluate bipolar reliability in mobile environments

2.1 Bipolar reliability according to uniform and non uniform distribution

We examine movement of nodes in two mobile models: random way points (RWP) [1] and Smooth mobile models (SMM) [2]. RWP and SMM correspond to uniform and non uniform node distribution in simulation area

In RWP model, the initialization nodes will pause for a certain period of time. Then they start moving in simulation area at a given average speed at a time. After the nodes reach their destination, they will pause at their position at some random time, called pause time. Then, the nodes select other random targets in simulation area and move there. The whole process repeats until simulation ends. If a button touches simulation edge during the move, it will bounce back to simulation area at the same speed and at an angle equal to its edge. RWP leads to distribution of non uniform nodes in simulation area. In other words, SMM maintains a uniform node distribution in survey area. SMM model follows physical law of smooth motion, each node movement has three phases: speed-up phase α, middle-smooth phase β, and slow-down phase γ. For each motion, a node selects a target direction θ and a target speed υ. At phase α, a node increases its speed uniformly until it reaches target speed υ. After that, the node maintains its speed and direction around value of target υ and υ during the β phase. At phase γ, its speed reduction node at steps γ until it stops completely. After each motion, the node still stops at its position with pause time. After pause time, a new direction and one speed button and repeat the three motion phases [6], [7].

We investigate Ad hoc networks including 11 nodes. Data transmission range of wireless nodes is chosen as 30m and the source and destination nodes are fixed respectively at $(x_0 = 0, y_0 = 50)$ and $(x_{11} = 100, y_{11} = 50)$. Therefore, at least four hops are needed to create a path between source node and destination node. When each node has a data transmission range of 30m, the total coverage by 11 nodes is three times survey area. All nodes, except power button and destination button, will be replaced at random in the 100m x 100m area at the time of simulation. Power button and destination button have a fixed position and are determined during simulation. When nodes start to move, bipolar reliability is expected to change. In this simulation, we will show how bipolar reliability is affected by mobile model of nodes. For each simulation scenario, simulation time is 500 seconds, and the results are obtained through average values from 100 different runs with different initializations. We assume that all nodes have same hardware platform and perform the same network tasks, exchange hello messages, etc. Therefore, all nodes have same reliability with corresponding time. We assume that a link between any two nodes has an operating probability of 0.9, regardless of distance between nodes. The environment and simulation parameters of Ad hoc networks are given as shown in Table 1:

Table 1. Parameters and constants are used in simulation

Space of length	Space of flatness 100 x 100
Number of nodes	11
Average node speed	10 and 20 (m/s)
Node mobility	RWP and SMM
Run time simulation	500 seconds
Node pause time	5 seconds
Data transmission range	30 m

We find that uniform node distribution is better than the non uniform node distribution. Non uniform node distribution leads to concentration of nodes in certain areas of survey area, at center of data network will lead to less paths dividing between connection nodes. In other words, uniform distribution allows more distributed paths between source and destination nodes and that increases reliability of data network to avoid errors. However, mobile model maintains consistent node distribution results with better data network reliability as shown in Figures 1 and 2.

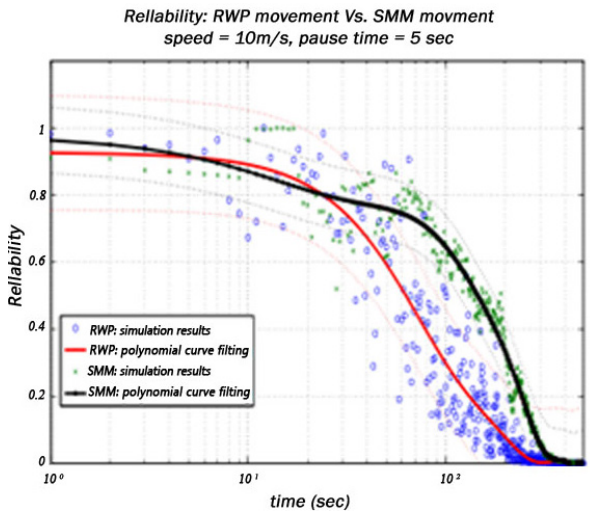

Fig. 1. Compare bipolar reliability according to RWP and SMM with Speed=10m/s and Pause Time=5s

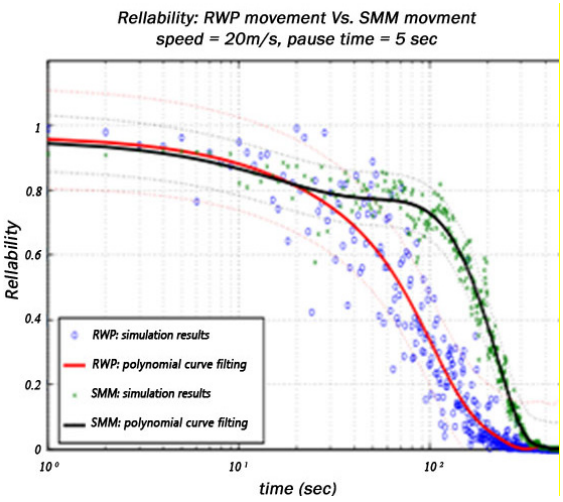

Fig. 2. Compare bipolar reliability according to RWP and SMM with Speed=20m/s and Pause Time=5s

Clearly we see that mobile model has an impact on data network reliability. First, the relationship between mobile matrices and bipolar reliability can be investigated through influence of these matrices on connection parameters of data network. There is a clear correlation between average level of node, average relative speed, average link duration and reliability of network. With distribution of similar spatial nodes according to given mobile model, if mobile model has a relatively high speed, the nodes can move from each other data range faster. Therefore, the lower connection duration occurs more frequently, which reduces number of distributed paths lower than bipolar reliability between source and destination nodes.

This effect is less serious than SMM due to physical limitations of moving node according to SMM. The speed of mobile node changes slightly rather than abruptly, so speed of current node depends on previous velocity. Accordingly, node positions together will not encounter major changes in a short time according to SMM. Therefore, a connection that exists between two nodes can maintain stability for a long time because nodes may be within each other's transmission range for longer periods. In other words, speed of the node at two different intervals does not depend on movement according to RWP. Therefore, position of RWP nodes changes dramatically for each other in any time period. These smooth and sudden changes in the position of nodes will affect bipolar reliability.

Figure 1 and figure 2 show that the reliability of SMM movement changes smoothly between two later time periods thanks to uniformly distributed nodes that have caused a spatial dependence among nodes as links between any two hops which keep stable values around their average one. In other words, RWP leads to sudden changes in reliability values between later times, because distribution of non uniform nodes causes the nodes to dominate in the middle of simulation area in almost time up. Therefore, the dependence of space between nodes is a location-dependent parameter, so the hops must not enter network center with a higher number of connections from points near the edges. Accordingly, the number of valuable paths between the two hop then changes quickly immediately.

2.2 Effect of node error rate on bipolar reliability and network performance matrix

Table 2. Constants and parameters used in simulation for networks in networks 6, 11, 18, 27 nodes

Space of length	Space of flatness 600 x 600
Number of nodes	6, 11, 18, 27
Average node speed	5, 10, 15, 20, 25, 30 (m/s)
Node model	Random way point
Run time simulation	500 seconds
Node stop time	5, 10, 15, 20, 25, 30 seconds
MAC class type	IEEE 802.11
Range of data transmission	250 m
Package number	1000 packages
Package size	1000 byte
Time interval between packages	0.5 seconds
Routing protocol	AODV

In this simulation, we first study effect of different error rates from nodes on network performance parameters such as packet loss rate and end-to-end control and delay messages. Then we present the effect of network performance on bipolar reliability.

We examine Ad hoc networks with 6, 11, 18, and 27 nodes placed in grid structure space of 600m×600m. Select the grid structure to ensure that high level of reliability can be achieved in each case. The wireless transmission range of selected nodes is 250m with a two-ray ground transmission model [3]. The environment and simulation parameters of Ad hoc networks are given in Table 2.

Error of a wireless node shows error of all wireless connections that occurred from that node. Therefore, terror of network topology warns nodes and network reliability. We examine effect of node error rate on some network performance parameters such as packet loss and control message loading. Because error rate increases, network is overloaded with control message and packet loss increases dramatically as shown in Figure 3 to Figure 6. The routing protocol tries to deal with the node error by finding new path among remaining node sets.

For bipolar reliability, with slow speed and large downtime, reliability of the network shows better stability. This is due to the stability of network routing for longer periods. As average speed of the mobile node increases, more connections will fail and that result in a few paths between source node and destination node as shown in Figure 7 and Figure 8. The bipolar reliability achieved from nodes moving at 5m/s with a stop time of 5 times better than moving nodes with 20-30m/s to 60% on average.

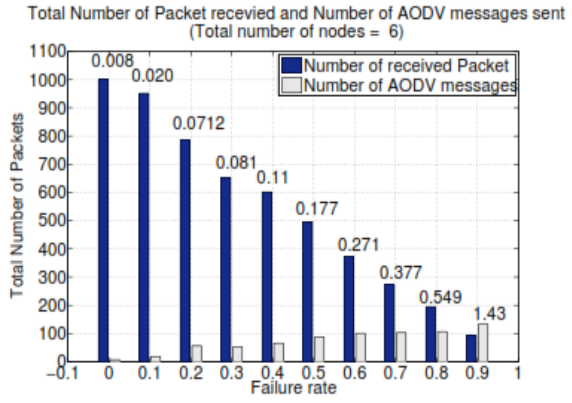

Fig. 3. Effect of node error rate and node sensitivity on network performance for 6-node network

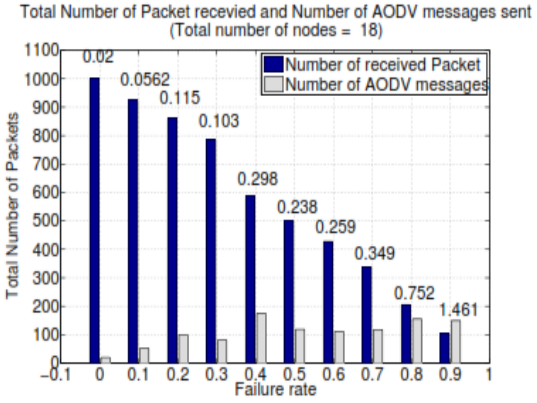

Fig. 5. Effect of node error rate and node sensitivity on network performance for network of 18 nodes

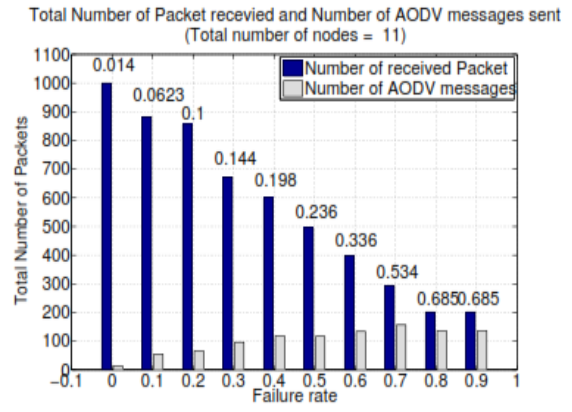

Fig. 4. Effect of node error rate and node sensitivity on network performance for 11-node network

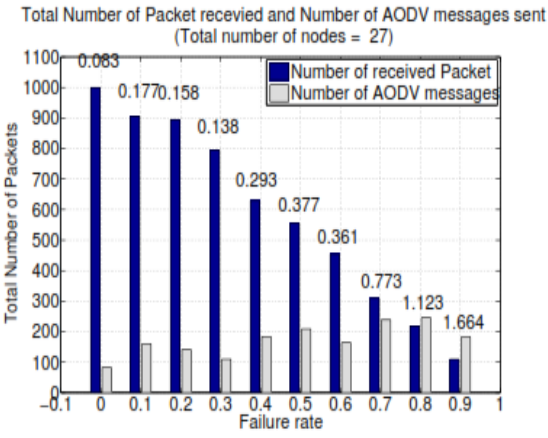

Fig. 6. Effect of node error rate and node sensitivity on network performance for network of 27 nodes

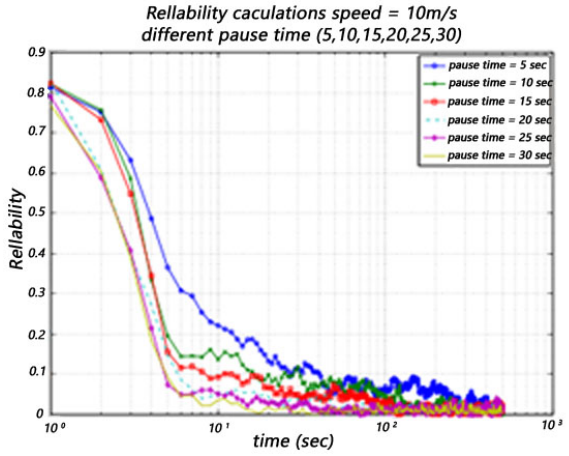

Fig. 7. Effect of node motion model on bipolar reliability: different node speed.

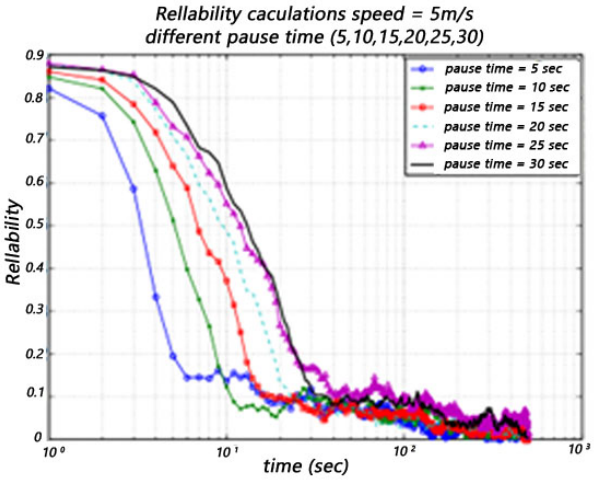

Fig. 8. Effect of node motion model on bipolar reliability: different stopping time.

On another aspect, nodes with a stop time greater than 20s are not much affected by increased movement speed because all nodes are relatively static for most of the time. We note that the error nature of components in a uniform wireless network affects shaping and extending the overall network reliability. The reliability of the attenuation node is an exponential function of time as in equation (3) due to battery power decline. Therefore, the overall reliability will be similar.

$$R_i(t) = e^{-(t/\lambda(t))^{\beta(t)}} \quad (3)$$

When speed increases from 5m/s to over 20m/s with 60% medium, loss of bipolar reliability value. In other words, because the downtime exceeds 20s, there is no significant increase in bipolar reliability and the increase in speed of the nodes is negligible. We have also shown the effect of uniform distribution and inconsistency to bipolar reliability of data network.

3. Detection method

Detection concept is a security mechanism that helps security personnel traces the source of the intrusion. Because information system components participate in a variety of processes with different functions, data transfer and organization, the detection technology is often integrated into two special levels: host and network. The storage level maintains an open search field. Tracing at operating system and network level allows to identify the intrusive information at the same level at which tracing techniques are availably performed. For example, network level detection techniques use network protocol sets or some unique field values such as averages for intrusion detection. However, at system level, additional information related to processing operations can be used for intrusion detection. This detection technique shows more details about intrusion because it focuses on how the compromised system works and when it is compromised to handle malicious code.

Trace techniques operate at system level

In system-level operation, surveyors need to analyze and reconstruct the system operations in order to identify certain risks and the methods used to attack the host, as well as effect of the risks on the system. There are a lot of sources of tracking at system-level operation to identify the risks, which are mainly caused by dynamic link libraries to run services and applications, but log file is the main one.

Exploitation and source processing services such signs often exploit operations at the application level. While output of such services is diverse, it limits the level of detail and only allows the survey of related events in application processing with a few selected properties required by admin. In addition to this limitation, the operation of the services can be changed by an intrusion or even paralyzed when the system is compromised because it runs at the host level.

In addition, the approach only allows for detection of changes to files and cannot handle intrusion but aims to change the operation of damaging execution processes. Exploiting at network level can reduce such problems because it can detect socket operations but it cannot provide a signal of confidence when requesting encryption mechanisms. Even assuming that detection is not encrypted, they may have to add intrusion operations such as insertion and evasion [4], [5], [7].

In order to conceal the weaknesses of the two exploitation approaches, some of the exploitation techniques developed further, implemented at the Operation System (OS) at the central level, have been proposed for several years. These detection solutions are based on some practical aspects with system-level operations such as system calls, signal selection in the way of system events including future file changes, terminal processing, internal data transfer, and memory usage. Exploitation at this level provides independence from related applications, and allows reliable surveys.

4. Conclusion

We studied the problem of calculating bipolar reliability in Adhoc network. We see that the mobile model affects data network reliability. Smooth and sudden changes in the position of nodes will affect bipolar reliability. For bipolar reliability, with slow speed and large downtime, the reliability of the network shows better stability. We have also shown the effect of uniform distribution and inconsistency to bipolar reliability of the data network. We have proposed a system-level traceability solution, additional information related to processing operations can be used to detect intrusion. This detection technique shows more details about intrusion because it focuses on how the compromised system works and when it is compromised to handle malicious code.

References

[1]. Sundararaman Jeyaraman and Mikhail J.Atallah, An empirical study of automatic event reconstruction systems, Digital Investigation, 3 (Supplement – 1):108-115, 2006

[2]. P.Garcia-Teodoro, J.Diaz-Verdejo, G.Macia-Fernandez, and E.Vazquez, Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers & Security, Vol.28, pp. 18-28, 2009.

[3]. A.G.Pennington, J.D.Stunk, J.L.Griffin, C.A.Soules, G.R.Goodson, and G.R.Ganger, Storage-based instruction detection: Watching storage activity for suspicious behavior, Proceedings of the 12th USENIX Security Symposium, 2003

[4]. V.Stavridou, B.Dutertre, R.A.Riemenschneider, and H Saidi Intrusion tolerant software architectures, DARPA Information Survivability Conference & Exposition II, DISCEX ’01., volume 2, pages 230-241, Anaheim, CA, USA, 2001.

[5]. B. Mukherjee, L. T. Heberlein, and K. N. Levitt, Network intrusion detection, Network, IEEE, vol. 8, no. 3, pp. 26–41,1994.

[6]. J. Z. Lei and Ali Ghorbani, Network intrusion detection using an improved competitive learning neuralnetwork, in Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR04), pp. 190–197.IEEE-Computer Society, IEEE, May 2004.

[7]. Deepika P Vinchurkar and Alpa Reshamwala,A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012.