An Investigation of Selfishness Attacks and Selective Forwarding Attacks in Mobile Ad Hoc Networks

Thongchai Chuachan[1]* and
Somnuk Puangpronpitag[2]

Abstract

Currently, there are several open research issues in Mobile Ad-hoc Networks (MANETs). However, previous studies are mainly focused on the routing robustness, scalability and survivability. There are several available attacking methods to MANETs. For MANET security investigation, we have selected Optimal Link State Routing (OLSR) and Open Shortest-Path First–MANET Designated Router (OSPF-MDR) protocols to evaluate the two critical types of attacks. The first one is a selfishness attacking. The second one is a selective forwarding attack. Experimental results have illustrated that OLSR and OSPF-MDR are vulnerable to the selfishness attacking and the selective attacking method.

Keywords : MANETs, selfishness attacking method, selective forwarding attack, performance evaluation, OLSR, OSPF-MDR, CORE emulator

[1] Department of Computer Science, Faculty of Science, SurindraRajabhat University
*E-mail: thongchai@srru.ac.th
[2] Department of Computer Science, Faculty of Informatics, Mahasarakham University
E-mail: somnukp@msu.ac.th

Introduction

In the future of network era, wireless entities are essential features for the network connectivity. Mobile Ad Hoc Networks (MANETs) (Corson & Macker, 1999) is one of the most important parts. MANETs can be acted as a router and a normal user. Moreover, MANETs automatically organize and form network structures. Routing protocols are important mechanisms to operate MANETs. In addition, two main functionalities have been normally used to describe routing characteristics including reactive and proactive routing protocol. In the reactive routing protocol, a protocol activates routing operations on-demand. In the proactive routing protocol, a protocol actively maintains routing paths for all known destinations. In particular, proactive routing protocols have been widely indicated as a good responsiveness to the topology changes. To explore such capabilities, two proactive routing protocols have been selected to use in study. The first one is the Open Shortest Path First–MANET Design Router (OSPF-MDR) (Ogier and Spagnolo 2009). The second one is the Optimized Link State Routing (OLSR) (Clausen & Jacquet, 2003).

A MANET nature undoubtedly shares medium accesses, and is easily to eavesdrop and to intercept sensitive information. Previous studies (Karlof & Wagner, 2003; Wu et al. 2007; Vasserman & Hopper, 2013) on MANET securities show several types of the attacking methods. Two of the most potential attacking methods are a selfishness attacking and a selective forwarding attack. In the selfishness attacking, malicious users always discard routing messages to avoid being an intermediate node. In the selective forwardingattack, attackers propagate themself as one of a traditional node. The attackers then attempt to be a part of the intermediate nodes, and drop data packets. Such attacking methods have caused legitimate users in MANETs, and have been selected in this study.

Three main evaluation methods, namely simulation, emulation and field-testing play an important role for MANET testing. The simulation tools such as NS-2 (The Network

Simulator-Ns-2), NS-3 (Network Simulator 3) and OMNeT++ (OMNeT++) typically run on a single machine, and simulate the operating system and protocols in abstract. Without rigorous statistical analysis, the simulation results inevitably lack of the scientific confidence (Millman, Arora, & Neville, 2011). Emulation is more accurate than simulation (Acosta & Medina, 2012), but it uses a long time an experiment. The field-testing actual hardware and software are used, but it normally tests after the intensive evaluation (Acosta & Medina, 2012). To achieve this work Common Open Research Emulator (CORE) (Common Open Research Emulator (CORE)) has been selected as a tool to perform realtime test-beds. CORE provides graphical user interface, and comprises lightweight virtual machines. In addition, each virtual machine is run by actual routing software, including Quagga Routing Suit (Quagga Routing Suite) and NRLOLSR (The NRL OLSR Routing Protocol Implementation). For experimental designs, static and dynamic scenarios have been used to study OSPF-MDR and OLSR against our selected attacking methods. In static scenarios, we can investigate capabilities of the routing maintenance. For dynamic scenarios, we can examine a routing convergence in critical situations. Experimental results demonstrate that OSPF-MDR outperforms OLSR for all attacking methods.

This paper is structured as follows. Section 2 is background. Section 3 is the experimental setup. Section 4 is the experimental results, and concludes in section 5.

Background

OSPF-MDR

Open Shortest Path First–MANET Design Router (OSPF-MDR) (Ogier & Spagnolo, 2009) is an extension of the Open Shortest Path First (OSPFv3) to support MANET. OSPF-MDR proactively operates to maintain all known destinations. MANET Designated Router (MDRs) is a key feature of OSPF-MDR, and provides better robustness and better response to topology changes. MDRs are constructed within 2-hop neighbor, and also form a Connected Dominating

Set (CDS). In addition, HELLO message is used to report neighbor states. A closed key feature is Backup MDR (BMDR), which is provided for backup a failure of MDRs. A node can select itself as an MDR if a value of Router Priority (RtrPri) is larger than the others.

OLSR

Optimized Link State Routing (OLSR) (Clausen & Jacquet, 2003) protocol operates as a proactive routing protocol. As in OSPF-MDR, OLSR maintains paths for all known destinations. A key feature of OLSR is the Multiple Point Relay (MPR). MPR mechanism can be used to avoid the duplication of routing nodes, and can reduce transmissions of the broadcast packets. Also, HELLO messages have been used to detect neighbors and links. In contrast to a traditional link state algorithm, it normally faces with network overhead. OLSR do not degrade network performance in a high node motility and density. OLSR and OSPF-MDR have been previously evaluated by Fang and his colleagues (Fang & Goff 2010). Experimental results show OLSR outperforms OSPF-MDR. However, security issues have not been investigated. In this paper, we further study the security issues on OSPF-MDR and OLSR.

MANET Routing Attacks

MANET routing protocols have been used in practical implementation (The NRL OLSR Routing Protocol Implementation); however, the attacking on MANETs are not rigorously investigated. (Wu et al., 2007) has thoroughly surveyed on the MANETs routing attacks, and classifies the attacking methods into two major categories. One is a passive attack and the other one is an active attack. The passive attack consists of Eavesdropping, Traffic analysis and Monitoring. To attack MANETs, attackers quietly eavesdrop and filter for sensitive information. While in the active attack, attackers normally involve interruption and modification (such as Jamming, Spoofing, Modification, Replaying and DoS). Currently, dangerously attacking methods almost appear in the active attacking methods including a selfishness attacking method and a selective forwarding attack.

Selfishness Attacks

A single user does not tend to cooperate with the others. The user normally avoids being intermediate node by discarding routing messages. In doing so, a sender is required to repair for a new routing path. Therefore, path discovery delay can be used to compare between OLSR and OSPF-MDR.

Selective Forwarding Attacks

A selective forwarding attack mainly thwarts data transmission between a sender and a receiver. An attacker is necessary to be a part of the intermediate nodes, and then refuses to relay data packets. In this study, the selective forwarding attack does not involve in a modification of the routing messages. An attacker only moves to the best location, and becomes a part of the intermediate nodes. For routing messages, the attacker normally cooperates with the others. The attacker easily destroys data communication between the sender and the receiver, and cannot be detected as an attacker. Currently, the selective forwarding attack is considerably dangerous for MANET environments. However, a profound evaluation of the selective forwarding attack has not been adequately investigated. In this paper, the selective forwarding attack problem has investigated in OLSR and OSPF-MDER routing protocol.

CORE Emulator

Emulation is more accurate than simulations (Acosta & Medina 2012), and Emulators can provide real-time perform-ance comparisons (Jain et al., 2011). Common Open Research Emulator (CORE) is one of a striking emulator for network test-beds. CORE gives virtual machines, and emulates the network protocol. For realtime test-beds, CORE uses virtual MANET nodes that provide routing services. For CORE performance evaluation, Ahrenholz et al. (Ahrenholz, 2010) has previously been experimented. Ahrenholz’s experimental results are closed to the physical network deployment, and are useful in realtime test-beds.

Experiment Setup

This section begins with experimental scenarios of OLSR and OSPF-MDR. We have selected static and dynamic scenarios for this study.

Static Scenarios

A design of static scenarios requires different multi-hop routing. Hence, five critical network scenarios have been designed, as shown in Figure 1. Each network scenario consists of ten nodes, and deploys a sender, a receiver and three attackers. The sender and the receiver appear in rectangles. Attackers show in circles. Solid lines are possible routing paths.

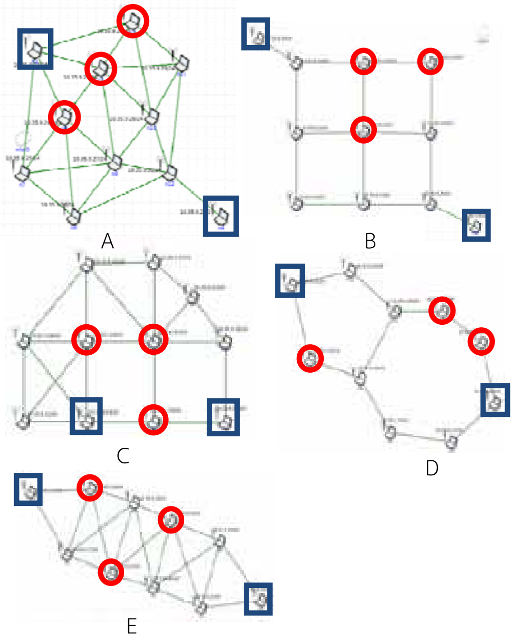

Figure 1. The network scenarios

Dynamic Scenarios

In dynamic scenarios, bonnmotion-2.0 has been used to randomize node positions and mobility speeds. We have controlled emulation parameters as shown in TABLE I. An emulation area is 700x700 meters. A mobility speed is random roughly 20m/s. A mobility model is Random Waypoint. There are 10 of network nodes to perform experiments and three of nodes are attackers.

TABLE I. PARAMETER SETUP

Parameters	Values
Area	700x700 m
Mobility speed	20m/s
Number of nodes	10
Mobility model	RandomWaypoint
MAC	802.11b

CORE Validation

Figure 2 shows a CORE validation scenario. Actual wireless hardware has been used to compare with CORE emulator. Extendable Mobile Ad-hoc Network Emulator (EMANE) (Extendable Mobile Ad-Hoc Network Emulator (EMANE)) has also been integrated with CORE because it is required to provide IEEE 802.11b. The expected results are approximated to IEEE 802.11b's theory as following. IEEE 802.11b, in theory, the maximum bit rate is 11Mbps. However, IEEE 802.11b data transmission requires the header control and the medium access control that require approximately 1687.81μs (Segata, Avancini, & Canton, 2009); thus, throughput at the application levels (a payload of 1047 bytes) is 1047x8bits/1687.81 or ≈6.97Mbps.

D-Link DWA-110 Wireless USB Adapter, Intel Core2 Duo E7300 2.66GHz with 3 MB caches, 2GB of RAM and 512GB disk are used in this validation testing. For a traffic generator, Iperf (The TCP/UDP Bandwidth Measurement Tool) has been selected to generate data traffic and to collect network statistics.

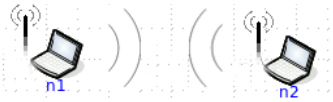

Figure 2. Validation Scenario

Attacking Model

We have selected a selfishness attacking method and a selective forwarding attack. For the selfishness attacking, users in MANETs avoid being an intermediate node by discard all routing messages. For the selective attacking technique, malicious users disguise to be a legitimate node, and reject to forward data packets for the others. We repeat the measurement to 30 runs. We mark experimental results with error bars of 95% confident interval. We use 6 minutes each experiment, and follow network events as in TABLE II.

TABLE II. NETWORK EVENTS

At (minute)	Action
2	Selfishness attacking
3	Normal situation
4	Selective forwarding attack
5	Normal situation
6	Halt

Network events in TABLE II are used in both static and dynamic scenarios. At the first two minutes, all MANET nodes are in a normal situation. Afterwards, for a minute, a selfishness attacking method have activated by using attacker nodes. At the third minute, we halt the selfishness attacking method. A minute later, a selective forwarding attack has been launched by the attacker node. At the last minute, we terminate CORE virtual nodes, and collect experimental statistics.

In our experiments, a Linux bash script has been developed as a node controller. Linux networking commands, namely tcpdump, timeout, iperf, iptables and vcmd are used by injecting those commands into CORE nodes. For example, three attackers require iptables to discard routing messages.

Experimental Results

This section demonstrates exper-imental results. For validation testing, 802.11b throughput generating by CORE has been compared with the throughput of real wireless hardware. For attacking results, we show OLSR and OSPF-MDR convergence time attacked by a selfishness attacking method and a selective forwarding attack.

CORE validation results

Experimental results of the hardware throughput are much lower than 802.11b's theory (generating by CORE), as shown in Figure 3. Roughly 1,000 runs, network throughputs of CORE emulator show approximately 6.6Mbps as in the 802.11b's theory. On the other hand, the throughputs of real wireless hardware present about 1.52Mbps, and have more variance than CORE emulator. The variation probably occur from the collision of the traffic in a real network environment. Thus, CORE emulator can show a precise network events.

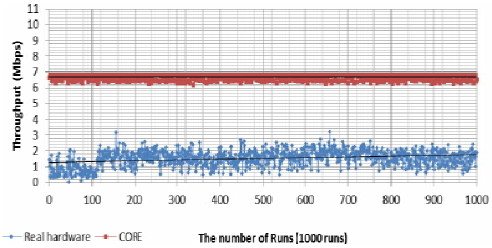

Figure 3. The throughput of the hardware and the emulator

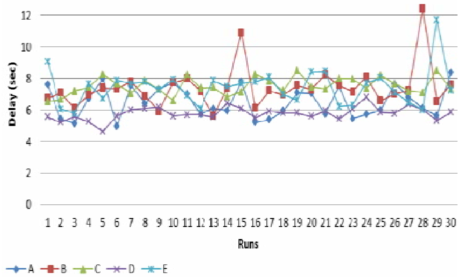

Figure 4. OLSR convergence time in static scenarios using the selfiness attacking method

Selfishness Attacking Results Static Scenarios

When OLSR suffers from a selfishness attacking method, it suddenly repairs a new routing path. As shown in Figure 4, A, B, C, D and E are our designed network scenarios. A convergence time of the five network scenarios demonstrates approximately 6.9±0.3 seconds. In general, OLSR operations always select the same routing path for a destination. Attackers can easily predict routing paths, and can find a location to attack against OLSR. However, a new suitable path is quickly repaired, and finally avoids the selfishness attacking method.

Figure 5 shows OSPF-MDR convergence time in each experiment. In the same network scenario, OSPF-MDR has selected a lot number of routing paths. For example, scenario B shows many different convergence time. Such values indicate that OSPF-MDR has selected a routing path without attackers to destroy user communication. A convergence time of the five network scenarios shows about 4.6±0.5 seconds. A benefit of the multiple designated routers in OSPF-MDR haveperformed better performance than OLSR for selfishness attacking environments.

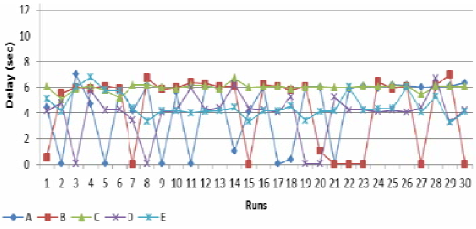

Figure 5. OSPF-MDR convergence time in static scenarios using the selective forwarding attack

Table III. A Routing Delay of Static Scenarios with 95% Confident Interval

Protocol	Routing delay (sec)				
	A	B	C	D	E
OLSR	6.5±0.3	7.4±0.4	7.5±0.1	5.7±0.1	7.4±0.4
OSPF-MDR	4.2±0.9	4.9±0.9	5.9±0.1	3.9±0.6	4.5±0.3

In distinct scenarios, shown in TABLE III., experimental results show that OSPF-MDR outperforms OLSR for all scenarios. OLSR are 6.5±0.3, 7.4±0.4, 7.5±0.1, 5.7±0.1 and 7.4±0.4 and OSPM-MDR are 4.2±0.9, 4.9±0.9, 5.9±0.1, 3.9±0.6 and 4.5±0.3 respectively. For analytical results, OSPF-MDR is more suitable to use than OLSR in the selfishness attacking environment.

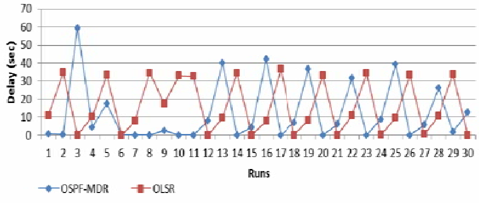

Figure 6. Convergence time of dynamic senarios using the selfiness attacking method

Dynamic Scenarios

Convergence time of dynamic senarios using the selfiness attacking method

For dynamic scenarios, Figure 6 shows convergence time after attacks using a selfishness attacking method. OLSR and OSPF-MDR have 15.9±5.2 and 11.8±5.9 seconds of convergence time. Consequently, OSPF-MDR outperforms OLSR to defend against the selfishness attacking method.

Selective Forwarding Attack Results Static Scenarios

In static scenarios, experimental results of the selective forwarding attack across five network scenarios demonstrate that OSPF-MDR and OLSR have failed to deliver data packets for a destination.

Attackers can easily select and drop the data packets. Fortunately, a few of data packet can be sent by using OSPF-MDR.

Figure 7 shows percentages of the packet delivery ratio (PDR) between OLSR and OSPF-MDR. OLSR is obviously unable to transmit data to a destination. OSPF-MDR shows approximately 30%, 32% and 23% in scenario A, B and E. A complete failure connection of OSPF-MDR in scenario C and D is from routing selection. The routing selection of the scenario C and D always passes attacker nodes.

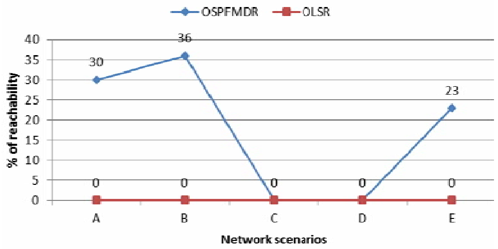

Figure 7. % of network reachability on the selective forwarding attack.

Dynamic Scenarios

In dynamic scenario, the PDR of OSPF-MDR and OLSR shows 80% and 70% respectively. A sender, a receiver and three attackers have been moved independently in an emulation region. In some cases, the sender and the receiver have resided nearby their transmission range. The attackers cannot thwart data transmission. Hence, the PDR in dynamic scenarios is higher that static scenarios. For both routing protocol in the selective forwarding attack, OSPF-MDR outperforms OLSR.

Conclusions

This paper aims to investigate the routing protocol capabilities against two critical types of MANET attacking methods. One is a selfishness attacking method and the other one is a selective forwarding attack.

We have selected two proactive routing protocols namely, OSPF-MDR and OLSR.

Selfishness attacking results show that OSPF-MDR outperforms OLSR in static and dynamic scenarios. For a selective forwarding attack, experimental results illustrate that OLSR is much weaker than OSPF-MDR in static and dynamic scenarios. In conclusion, OSPF-MDR is suitable to use in critical MANET environments.

References

Acosta, J. & Brenda, M.(2012).Survivability Prediction of Ad Hoc Networks Under Attack. In Orlando, Florida, USA.

Ahrenholz, J. (2010). *Comparison of CORE Network Emulation Platforms*. San Jose, California, USA, 166-171.

Clausen, T. & Philippe, J.(2003). Optimized Link State Routing Protocol (OLSR). *RFC*, 3626.

Common Open Research Emulator (CORE) http://www.nrl.navy.mil/itd/ncs/products/core, accessed June 16, 2014.

Corson, S. & Joseph, M. (1999). Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC, 2501.

Extendable Mobile Ad-Hoc Network Emulator (EMANE) http://www.nrl.navy.mil/itd/ncs/products/emane, accessed June 16, 2014.

Fang, J. & Tom, G. (2010). Comparison Studies of OSPF-MDR, *OLSR and Composite Routing*. In 989–994.

Jain, K., Ayan Roy-C., Kiran, S., Baobing ,W., & John, B. (2011). *Studying Real-Time Traffic in Multi-Hop Networks Using the EMANE Emulator: Capabilities and Limitations*. In 93–95. Barcelona, Spain.

Karlof, C. & David, W. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *InWorkshop on Sensor Network Protocols and Applications*. 113–127.

Millman, E., Arora, D., & Neville, S. (2011). STARS: A Framework for Statistically Rigorous SimulationBased Network Research. In 733 – 739. Biopolis, Spain.

Network Simulator 3. (2014). http://www.nsnam.org, accessed May 17, 2014.

Ogier, R. & Phil, S. (2009). Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding. *RFC*, 5614.

OMNeT++.(2014). http://www.omnetpp.org/, accessed May 17, 2014.

Quagga Routing Suite. (2014). http://www.nongnu.org/quagga/, accessed June 16, 2014.

Segata, M., Mattia, A., & Chiara, C. (2009). Measuring Throughput of 802.11 B and G Protocols. Technical Report.

The Network Simulator - Ns-2. (2014). http://www.isi.edu/nsnam/ns/, accessed May 17, 2014.

The NRL OLSR Routing Protocol Implementation. (2014). http://www.nrl.navy.mil/itd/ncs/products/olsr, accessed June 16, 2014.

The TCP/UDP Bandwidth Measurement Tool. (2014). http://iperf.fr/, accessed May 10, 2014.

Vasserman, E., and Nicholas H. (2013). *Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks, 12*(2), 318–332.

Wu, B., Jianmin, C., Jie, W., & Mihaela, C. (2007). *A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks*, 103–135.