TRUST BASED FLOODING ATTACK DETECTION AND RESPONSE MECHANISMS FOR AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

BAHRAM YAGHOUBZADEH ASHOURUAN

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

This project report is dedicated to my beloved wife, father, mother and sister for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my valued supervisor **DR. SHUKOR ABD RAZZAK** for his constant support during my study at UTM. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor.

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities to complete my master program and this project.

ABSTRACT

Mobile Ad hoc Networks provide a structure-less environment, enabling participants in the coverage mobile nodes to communicate each other without using any centralized authentication agent. Thus, it is compromised in face to various sorts of attacks. Unfortunately, none of the presented secured routing protocols can detect internal Denial of Service (DoS) attacks by itself naturally. One of the most important and effective internal misbehaviors which has dramatic side effects on the network's throughput is Flooding Attack. This project aims at proposing an alternative solution to detect and respond Flooding Attack in MANET which is based on cooperative trust evaluation mechanisms. Actually, this approach is matched to basic principles of distributed networks in which the participating nodes are responsible for any needed creation, operation and maintenance of the network. Moreover, it seems useful for high mobility networks where the suspicious nodes move around the area repeatedly. Consequently, the gained results of the project prove that the proposed Trust-based Cooperation mechanisms decreases the side effects of Flooding Attack on Ad-hoc On-demand Distance Vector routing protocol.

ABSTRAK

Rangkaian Segera Bergerak (Mobile Adhoc Network) menyediakan persekitaran kurang berstruktur, membolehkan pengguna yang berada di dalam kawasan liputan untuk berkomunikasi di antara satu sama lain tanpa menggunakan sebarang agen pengesahan berpusat. Oleh itu, ia mampu berhadapan dengan pelbagai jenis serangan. Malangnya, tiada satu pun protokol laluan keselamatan tersebut dapat mengesan Denial of Service (DOS) dalaman yang diserang oleh diri sendiri secara semulajadi. Di antara kepentingan dan keberkesanan tingkahlaku dalaman yang memberi kesan sampingan kepada laluan rangkaian ialah *Serangan Banjir* (Flooding Attack). Projek ini bertujuan untuk mencari penyelesaian alternatif bagi mengesan dan bertindakbalas dengan *Serangan Banjir* dalam MANET yang mana ia berteraskan mekanisma penilaian kepercayaan kerjasama. Sebenarnya, pendekatan ini berpadanan dengan asas prinsip kepada rangkaian yang beredar / bergerak di mana node atau laluan yang turut serta adalah bertanggungjawab kepada sebarang keperluan yang dicipta, pengoperasian dan penyelenggaraan kepada rangkaian. Selain itu, ia sangat berguna untuk rangkaian bergerak yang tinggi di mana node yang mencurigakan bergerak mengelilingi kawasan tersebut secara berulang-ulang. Kesimpulannya, hasil keputusan yang diperolehi dari projek ini membuktikan bahawa cadangan mekanisma Trust-based Cooperation dapat mengurangkan kesan sampingan *Serangan Banjir* (Flooding Attack) kepada protokol laluan On-Demand Distance Vector.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AMTT	Avoiding Mistaken Transmission Table
AODV	Ad hoc On-Demand Distance Vector
ARAN	Authenticated Routing for Ad-hoc Networks
DOS	Denial of Service
DSDV	Destination-Sequenced Distance-Vector Routing
DSR	Dynamic Source Routing
FAP	Flooding Attack Prevention
FIFO	First in First Out
MANET	Mobile Ad hoc Network
MS	Microsoft
NS2	Network Simulation ver.2
PRP	Proactive Routing Protocols
RAD	Random Assessment Delay
RREP	Route Reply
RREQ	Route Request
RRER	Route Error
RRP	Reactive Routing Protocols
SAODV	Secure Ad hoc On-Demand Distance Vector
SEAD	Secure Efficient Ad hoc Distance Vector Routing Protocol
SMRTI	MANET Routing with Trust Intrigue
WEP	Wired Equivalent Privacy
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Overview

Today, Mobile Ad-hoc Networks (MANET) have been popular because of its exclusive characteristics which have allowed wireless devices to connect each other easily when fall in the radio coverage of each other [1]. Also, each node performs the roles of an end-system and works also as a router to forward packet through the network; therefore, mobile ad hoc network uses the concept of multi hop communication. In addition, every node can move in the network freely. This mobility is as a result of dynamic topology in MANET without any infrastructure requirements such as centralized access point or centralized administration. As a result, each node is in charge of its security threats [2]. Actually, the lack of infrastructure in MANET nominates this kind of networks for using wherever the implementation of network infrastructure is impossible or too expensive such as military usages, emergency applications, PDA networking, and usual applications such as wireless meeting or classroom.

MANET uses routing protocols to route packets to destination like the conventional wired networks which are divided into PRP (Proactive Routing Protocol) and RRP (Reactive Routing Protocol) [3, 4]. Proactive Routing Protocols is called Table Driven Routing Protocol too. In PRP the routing information of all nodes are stored by the others, and routing updates are propagated whenever the topology of the network changes [5]. Another side, in the case of RRP, route

between the nodes is searched only whenever a source node wants to communicate with the others; they use Flooding method to discover the route by sending route request message which will be replied by the purposed destination. But the method of on-demand routing to facilitate route discovery may be used by the Intruders or the malicious node to consume the network resources, leading to Flooding attack [6, 7].

The remaining of this chapter is organized as follows; the second section will be discussed problem background, subsequently, problem statement will be described; the rest of the chapter is allocated for the objectivity of the project and its scope; finally, significant of the project and references are cited.

1.2 Problem background

According to properties of MANET, especially the lack of network infrastructure such as centralized administration, every node consists of many sorts of attacks; mostly, denial of service attacks. Although, using RRPs (On demand Routing Protocols) have irrefutable benefits for mobile ad hoc network, however, they increases the risk of DoS attacks.

Actually, like conventional wired networks, MANET uses routing protocols to forward packets to the destination; Proactive routing protocols also, known as table-driven protocols is based on routing table between nodes. However, the main advantage of Proactive routing protocols can be declared as predictability of the control over head on these protocols; since it has a fixed upper bound which enables it to be independent to the traffic profiles [22]. In contrary, as disadvantages, we can state that they are not scalable perfectly and maintenance of routing table requires substantial network resources [20]. On the other hand, Reactive routing protocols or on-demand routing protocols are developed for MANET to direct packets to the destination. In fact they indicate the real basis of MANET which provides more

dynamic networks in comparison with structured ones. In the on demand routing protocols, nodes search for a route when they want to communicate with each other. To discover the routes they use route discovery procedure which in turns uses the Flooding method. Therefore, updating of the routing information is presented whenever a node requires a route instead of periodically updating the route information. Consequently, the control overhead will be reduced, especially in high mobility networks where the periodical update causes significant waste overhead [22]. However, on demand, routing protocols are categorized into secured on demand routing protocols such as SAODV [29], SEAD [32], SRP [21], ARAN [2], and Adriane [30]. And non-secure on demand routing protocols such as AODV [11] and DSR [23]. According to the studies, AODV is one of the most popular routing protocols for implementing additional DoS Attack detection modules because of its dynamic structure and perfect performance [12, 13].

In fact, MANET Flooding Attack is known as a harmful DoS attack which affects on functionality of almost all RRPs sharply. Mobile Ad hoc Flooding attack makes it possible for an adversary to carry out DoS by saturating the support with a quantity of broadcasting messages, by reducing the output of nodes, and in the worst case, to prevent them from communicating. In fact, there is similar attack in conventional wired networks which is popularly called SYN Flooding attack. In this attack, the attacker sends many TCP connection requests with spoofed source addresses to a victim. As a result, the resources of the victim host will be exhausted; subsequently, no more incoming TCP connection can be established by this machine [8].

Before describing Flooding Attack in MANET, it seems necessary to describe more about on-demand protocols especially AODV [11] which this project is relied on. AODV is one of the on-demand routing protocols, designed for MANET to manage unicast, multicast, and broadcast announcement. Actually, AODV is developed by using some principles of DSR [23] and DSDV [24] which are route discovery and route preservation from DSR and hop by hop steering sequence number and sporadic beacons from DSDV, respectively.

Actually, Flooding attack in MANET is categorized to two types which are Route Request (RREQ) Flooding attack and Data Flooding attack [8]. In RREQ Flooding attack the attacker broadcasts many route requests without consider to Rate-Limit, roundtrip-time, and Back-off-time. On the other hand, Data Flooding Attack occurs when an attacker creates a communication path with a victim node; and in the next step sends a huge amount of useless data packets to it to exhaust recourses of all intermediate nodes and waste bandwidth of the network. Because of the authentication methods implemented in on-demand protocols, the intermediate nodes cannot understand the contents of the packets, but they can just forward them to the destination; therefore, no one can detect data Flooding attack except the application layer of destination node [8].

Many valued efforts for sure have been tried to mitigate Flooding attack in MANET by using vary approaches such as FAP [8], AMTT [14], Filtering scheme [9, 10], and Trust scheme; but consequently, it seems that none of the mentioned mechanisms could solve Flooding attack in MANET totally. In fact, each of them has its specific limitations to solve both types Flooding Attack which will be described comprehensively in the rest of this article. However, this project proposes an alternative trust based scheme which is combination of related solution's strength and it is relied on cooperation between friend nodes. The main idea of this approach is coming from a friendship based framework [44, 45]; in the proposed scheme, we try to collect trust values from two ways as direct trust estimation and indirect trust value (Recommended trust) which are coming from friend neighboring nodes with a coefficient value that indicates their efficiency level in the decisions.

1.3 Problem statement

Although, Flooding Attack does not use any complex process to flood network, but the secured routing protocols cannot detect this attack naturally. This research tries to use a trust based mechanism to response route request Flooding Attack in MANET according to neighbor suppression approach. Moreover,

cooperative mechanism to collect information about suspicious nodes can restrict them for long term in the virtual societies greatly; then the problem of stranger nodes in high mobility situations can be solved too. Furthermore, this cooperation is based on both direct and indirect trust evaluation approach which is introduced as a suitable approach for distributed networks such as MANET or WSN [38]. This research will tries to show that cooperation of friend nodes can develop a trusted set of nodes which can help to each other to make the best decision about a suspicious node and limiting its capabilities to Flooding area by using both direct trust calculating and recommended (indirect) trust computing simultaneously.

1.4 Aim of the project

This project tries to detect MANET Flooding attack by proposing a trust based mechanism as an alternative solution and also response side effects of this internal misbehavior.

1.5 Objectives of the project

In order to mentioned aims of the project, the objectives of the project related to flooding problem in MANET are stated as below:

- To analyze existing problems and solutions in MANET, related to Flooding attacks.
- To design alternative solution for MANET Flooding attack problem by using trust based mechanisms.
- To evaluate trust based Flooding Attack detection and response mechanisms for Ad hoc On-demand Distance Vector routing protocol.

1.6 Scope of project

The scope of this project is defined as following:

- Evaluations will be conducted only in simulation.
- Trust based Flooding Attack detection and response mechanisms will be compared with the original AODV routing protocol.

1.7 Significance of the study

The outcome of the project is to detect route request Flooding attack by using an enterprise trust based mechanism which controls active nodes of MANET to detect and response Flooding Attack. Actually, this method works as a friendship system to identify suspicious senders for long term and decrease the side effects of their attacks by monitoring their propagation. This project aims at introducing an alternative trust based mechanism to record background activities of vicious nodes and setup a plural opinion system for recognizing strangers in high mobility situation.

LIST OF REFERENCES

1. Lidong, Z. and Z.J. Haas, Securing ad hoc networks. *Network, IEEE,* 1999. 13(6): p. 24-30.
2. Sanzgiri, K., et al. A secure routing protocol for ad hoc networks. *in Network Protocols, 2002. Proceedings. 10th IEEE International Conference on.* 12-15 Nov. 2002. 78-87.
3. Royer, E.M. and T. Chai-Keong, A review of current routing protocols for ad hoc mobile wireless networks. *Personal Communications, IEEE,* 1999. 6(2): p. 46-55
4. Papadimitratos, P. and Z.J. Haas, Secure Routing for Mobile Ad Hoc Networks, *in Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*. 2002. p. 193-204.
5. Abolhasan, M., T. Wysocki, and E. Dutkiewicz, A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, 2004. 2(1): p. 1-22.
6. Kannhavong, B., et al., A survey of routing attacks in mobile ad hoc networks. *Wireless Communications, IEEE*, 2007. 14(5): p. 85-91.
7. Wu, B., et al., *A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*, in *Wireless Network Security*, Y. Xiao, X. Shen, and D.-Z. Du, Editors. 2007, Springer US. p. 103-135
8. Ping, Y., et al. Resisting flooding attacks in ad hoc networks. *in Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on.* 4-6 April 2005. 657-662 Vol. 2.
9. Jian-Hua S., et al. Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks. Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06). 2006

10. Desilva, S. and R.V. Boppana. Mitigating malicious control packet floods in ad hoc networks. *in Wireless Communications and Networking Conference, 2005 IEEE.* March 2005. 2112-2117 Vol. 4. P. 13-17
11. Perkins, C.E. and E.M. Royer. Ad-hoc on-demand distance vector routing. *in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on.* 25-26 Feb 1999. 90-100.
12. Perkins, C.E., et al., Performance comparison of two on-demand routing protocols for ad hoc networks. *Personal Communications, IEEE,* 2001. 8(1): p. 16-28.
13. Belding-Royer, E.M. and C.E. Perkins, Evolution and future directions of the ad hoc on-demand distance-vector routing protocol. *Ad Hoc Networks,* 2003. 1(1): p. 125-150.
14. Shaomei, L., et al. A New Method to Resist Flooding Attacks in Ad Hoc Networks. *in Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006.International Conference on.* 22-24 Sept. 2006. 1-4.
15. Venkataraman, R., et al., Prevention of flooding attacks in mobile ad hoc networks, *in Proceedings of the International Conference on Advances in Computing, Communication and Control*. 2009, ACM: Mumbai, India. p. 525-529.
16. Hu, Y.-C., A. Perrig, and D.B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, *in Proceedings of the 2nd ACM workshop on Wireless security*. 2003, ACM: San Diego, CA, USA. p. 30-40.
17. Venkataraman, R., M. Pushpalatha, and T. Rama Rao, *A Generalized Trust Framework for Mobile Ad Hoc Networks*, in *Recent Trends in Networks and Communications*, N. Meghanathan, et al., Editors. 2010, Springer Berlin Heidelberg. p. 326-335.
18. Pirzada, A.A. and C. McDonald, Establishing trust in pure ad-hoc networks, *in Proceedings of the 27th Australasian conference on Computer science - Volume 26*. 2004, Australian Computer Society, Inc: Dunedin, New Zealand. p. 47-54.
19. Theodorakopoulos, G. and J.S. Baras, Trust evaluation in ad-hoc networks, *in Proceedings of the 3rd ACM workshop on Wireless security*. 2004, ACM: Philadelphia, PA, USA. p. 1-10.

20. Shishir K Shandilya and Sunita Sahu, A Trust Based Security Scheme for RREQ Flooding Attack in MANET, in *International Journal of Computer Applications*, Volume 5– No.12, August 2010. P. 0975 – 8887.
21. Li Cui Zhang et al., Research of Secure Scheme Against Data Flooding Attack in Ad Hoc Networks, Advanced Materials Research, Volumes 204-210, 2011. P. 395-399
22. Z Chang, G. N. Gaydadjiev, S. Vassiliadis, Routing Protocols for Mobile Ad-hoc Networks: Current Development and Evaluation, *Proceedings of the 16th Annual Workshop on Circuits, Systems and Signal Processing*, ProRisc 2005, Veldhoven, the Netherlands, November 2005. p. 489-494,
23. Perkins, C.E. and P. Bhagwat, Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. *SIGCOMM Comput. Commun. Rev.*, 1994. 24(4): p. 234-244.
24. D.B. Johnson, D.A. Maltz, J. Broch, DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks, in *Ad Hoc Networking, Addison-Wesley*, 2001. pp. 139–172.
25. Balakrishnan, V., et al. Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications. *in Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on.* 27-30 Aug. 2007. 29-29.
26. Williams, B. and T. Camp, Comparison of broadcasting techniques for mobile ad hoc networks, *in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking \& computing*. 2002, ACM: Lausanne, Switzerland. p. 194-205.
27. Balakrishnan, V., et al. Trust Enhanced Secure Mobile Ad-Hoc Network Routing. *in Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on.* 21-23 May 2007. 27-33.
28. Kim, H., R.B. Chitti, and J. Song, Novel defense mechanism against data flooding attacks in wireless ad hoc networks. *Consumer Electronics, IEEE Transactions on*, 2010. 56(2): p. 579-582.
29. Zapata, M.G., Secure ad hoc on-demand distance vector routing. *SIGMOBILE Mob. Comput. Commun. Rev.*, 2002. 6(3): p. 106-107.
30. Hu, Y.-C., A. Perrig, and D.B. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.*, 2005. 11(1-2): p. 21-38.

31. Awerbuch, B., et al., An on-demand secure routing protocol resilient to byzantine failures, *in Proceedings of the 1st ACM workshop on Wireless security*. 2002, ACM: Atlanta, GA, USA. p. 21-30.
32. Hu, Y.-C., D.B. Johnson, and A. Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 2003. 1(1): p. 175-192.
33. Sudhir Agrawal, et al., A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks, *Journal of Computing*, Volume 3, Issue 1, January 2011. P. 41-48
34. Weimerskirch, A. and G. Thonet, *A Distributed Light-Weight Authentication Model for Ad-hoc Networks*, in *Information Security and Cryptology — ICISC 2001*, K. Kim, Editor. 2002, Springer Berlin Heidelberg. p. 341-354.
35. Chlamtac, I., M. Conti, and J.J.N. Liu, Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 2003. 1(1): p. 13-64.
36. Chlamtac, I., M. Conti, and J.J.N. Liu, Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 2003. 1(1): p. 13-64.
37. Corson, M.S., J.P. Macker, and G.H. Cirincione, Internet-based mobile ad hoc networking. *Internet Computing, IEEE*, 1999. 3(4): p. 63-70.
38. Kannhavong, B., et al. Analysis of the node isolation attack against OLSR-based mobile ad hoc networks. *in Computer Networks, 2006 International Symposium*. p 30-35.
39. Yan, S., H. Zhu, and K.J.R. Liu, Defense of trust management vulnerabilities in distributed networks. *Communications Magazine, IEEE*, 2008. 46(2): p. 112-119.
40. Balakrishnan, V., et al. Trust and Recommendations in Mobile Ad hoc Networks. *in Networking and Services, 2007. ICNS. Third International Conference on.* 19-25 June 2007. 64-64.
41. Sun, Y.L. and Y. Yafei. Trust Establishment in Distributed Networks: Analysis and Modeling. in Communications, 2007. ICC '07. IEEE International Conference on. 24-28 June 2007. 1266-1273.
42. Jie, L., L. Ruidong, and K. Jien, Future trust management framework for mobile ad hoc networks. Communications Magazine, IEEE, 2008. 46(4): p. 108-114.

43. Sterne, D., et al. A general cooperative intrusion detection architecture for MANETs. in Information Assurance, 2005. Proceedings. Third IEEE International *Workshop on*. 23-24 March 2005. 57-70.

44. Razak, S.A., et al., Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks. *Ad Hoc Networks*, 2008. 6(7): p. 1151-1167.

45. Razak, S. A. et al., A friend mechanism for mobile ad hoc networks, Journal of Information Assurance and Security, 4 (5), 2009. p.440-448.

46. Balakrishnan, V., V. Varadharajan, and U.K. Tupakula. Fellowship: Defense against Flooding and Packet Drop Attacks in MANET. *in Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*. 3-7 April 2006. 1-4.

47 Balakrishnan, V., et al. TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks. *in Networks, 2007. ICON 2007. 15th IEEE International Conference on*. 19-21 Nov. 2007. 182-187.

48. Ibrahim, M.M., N. Sadek, and M. El-Banna. Prevention of flooding attack in wireless ad-hoc AODV-based networks using Real-time Host Intrusion Detection. *in Wireless and Optical Communications Networks, 2009. WOCN '09. IFIP International Conference on*. 28-30 April 2009. 1-5.

49. Stamouli, L., P.G. Argyroudis, and H. Tewari. Real-time intrusion detection for ad hoc networks. *in World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*. 13-16 June 2005. 374-380.

50. Pahlevanzadeh, B. and A. Samsudin. Distributed hierarchical IDS for MANET over AODV&#x002B. *in Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on*. 14-17 May 2007. 220-225.

51. Bourkache, G., M. Mezghiche, and K. Tamine. A Distributed Intrusion Detection Model Based on a Society of Intelligent Mobile Agents for Ad Hoc Network. *in Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*. 22-26 Aug. 2011. 569-572.

52. Kumar N. et al., securing a mobile ad-hoc network from routing attacks through the application of genetic algorithm, arXiv1202.4628v1, 21 Feb 2012. 6 pages

53. Balakrishnan, V., et al. Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks. *in Wireless Communication Systems, 2007. ISWCS 2007. 4th International Symposium on.* 17-19 Oct. 2007. 592-596.

54. Kurkowski, S., T. Camp, and M. Colagrosso, MANET simulation studies: the incredibles. *SIGMOBILE Mob. Comput. Commun. Rev.*, 2005. 9(4): p. 50-61.

55. K.Fall and K.Varadhan, The *ns* Manual (formerly *ns* Notes and Documentation). November 4 2012