Selective Acknowledgement Scheme to Mitigate Routing Misbehavior in Mobile Ad Hoc Network

Nimitr Suanmali[1], Kamalrulnizam Abu Bakar[2] and Suardinata[3]

[1]Department of Computer System and Communication, Faculty of Computer Science & Information Systems, University Teknologi Malaysia, Johor Bahru, Malaysia
Suan Dusit Rajabhat University,Bangkok,Thailand

[2]Department of Computer System and Communication, Faculty of Computer Science & Information Systems, University Teknologi Malaysia, Johor Bahru, Malaysia

[3]Department of Computer System and Communication, Faculty of Computer Science & Information Systems, University Teknologi Malaysia, Johor Bahru, Malaysia
STMIK Indonesia Padang, Padang Indonesia

Abstract

Mobile Ad Hoc Networks (MANETs) rely on the preliminary hypothesis that all co-operating nodes completely cooperate in an infrastructureless wireless network. Each node helps each other to perform network functions in a self-organization way. However, some nodes in a network may oppose to cooperating with others to avoid consuming their battery power and other resources. Recently, the routing misbehavior has been an interesting topic in this research field. In this paper, we propose selective acknowledgement (SACK), an end-to-end network-layer acknowledgement scheme, which can be easily attached on top of all source routing protocol. Dissimilar all previous research attempts made to tolerate routing misbehavior, this study discloses the malicious action and then recognizes compromised node or malicious nodes in the network. The malicious node will be prevented in the future routing process to improve the performance of the network throughput. Additional information of SACK scheme and preliminary evaluation are presented in this paper.

Keywords: *Mobile Ad hoc Network, MANET, Selfish, Routing Misbehavior, Malicious, Non-cooperation, Reputation.*

1. Introduction

The growth of wireless computer networks plays increasingly vital roles in modern society. Self organization, lacks of infrastructure, and dynamic change of nodes are the main characteristic of Mobile Ad Hoc Network (MANET). A MANET is a collection of wireless mobile nodes performing a temporary network without any established infrastructure or centralized authority[1]. Such network does not rely on fixed architecture and pre-determined connectivity. Nodes transmit information directly to another in a range of their wireless signal. The transmission range depends not only on the power level used for the transmission, but also on the terrain, obstacles and the specific scheme used for transmitting the information[2]. Nodes in MANET are dynamically changed, which means that the topology of such networks may change rapidly and unpredictably over time. A MANET consists of devices that are autonomously self-organized into networks. A self-organizing capability makes MANET completely different from any other network. MANET is one of the most innovative and challenging areas of wireless networks. It is a key step in the evolution of wireless networks. The network is a self-organization which means that all network activity including discovering the topology and delivering messages must be executed by themselves, i.e., routing functionality will be incorporated into mobile nodes. An extensive description about the ad-hoc networks and the interrelated research topics can be found in [16][17][18][19][20]. The main challenge of MANET is the vulnerability to security attacks. The security challenge has become a primary concern to provide secure communication.

In MANETs, routing misbehavior can seriously downgrade the performance at the routing layer. Particularly, nodes may take part in the route discovery process and maintenance processes but deny to forward data packets. How do we disclose a misbehavior activity? How can we perform such a detection processes more effective, with low routing control overhead, and more accurate, with less false detection rate and false alarm?

In this paper, we concentrate on routing misbehavior that is a severe threat to Mobile Ad hoc networks. Although many research attempts have been proposed to secure routing protocols, but it is not adequately addressed for the routing

misbehavior. We have studied routing misbehavior in which a malicious node kindly forward a routing message but intentionally drops the data packets they received, unlike all previous research efforts made to tolerate routing misbehavior, our work detected the malicious activity and then identified the compromised nodes or malicious behavior nodes in the network. We propose a scheme called Selective Acknowledgement (SACK) to detect misbehaving nodes, which can be implemented on network layer of any source routing protocol. The source node validates that the packet forwarded is received completely by neighbor nodes on the source route by a specific type of acknowledgement packets, called SACK packets. SACK packets have a related operation as the SACK packets on the TCP layer, but the SACK packets in TCP are used for reliable communication and flow-control. A neighbor node noticed the arriving of data packet by reply back to the source node with a SACK packet. The neighbor node will suspect to be a malicious node, if the source node does not accept a SACK packet interrelated to a specific data packet that was replied back. The malicious node will be avoided in the future routing process, so the throughput performance of overall network will be enhanced.

The rest of the paper is organized as follows. In section 2, various approaches mitigated routing misbehavior are summarized. In section 3, the details of routing misbehavior are given. The information of the SACK system and interrelated discussion are presented in section 4. We conclude the work in section 5.

2. Related Work

The fundamental technique for the most of an intrusion detection system that found in this section is Watchdog. Sergio Marti et al. [3] proposed an intrusion detection technique called Watchdog and constructed on a Dynamic Source Routing (DSR) protocol [4]. The authors proposed two techniques to improve a throughput ratio in the situation that compromised nodes willing to forward routing packets but reject to forward data packets. The first technique is Watchdog, which recognizes misbehaving nodes while the second technique, the Pathrather, which is similar to an intrusion detection system that helps routing protocols to eliminate these misbehaving nodes from the active route. When a node forwards a packet, the node's Watchdog verifies that the next node in the path also forwards the packet by listening continuously in a promiscuous mode to the neighbor node's transmissions. If the neighbor node does not forward the packet, it was decided as a misbehaving node. The Watchdog increases the misbehaving counter every time a node misses to forward the packet. If the misbehaving counter reaches a particular threshold, it recognized that the node is misbehaving node, then this node is prevented using the Pathrather. The drawbacks of watchdog are that it might not detect a misbehaving node in the presence of receiver collision, ambiguous collision, false misbehavior reporting, limited transmission power, partial dropping and collusion.

Hasswa et al. proposed an intrusion detection and response system for mobile ad hoc network called Routeguard[5]. This technique is a combination of two techniques, Watchdog and Pathrather, proposed by Marti et al. [3], to categorize each neighbor node into 4 categories: fresh, member, unstable, suspect. The Watchdog classified each node based on the ratings acquired from its behavior. Moreover, each category has a various trust level as trusted and untrusted. The trusted member lets the node to take part in the network. On the other hand, the untrusted member corresponds to a node that is absolutely untrusted and not allowed from using the network resources. Routeguard is a similar process to the Pathrather which performs by every node in the network and takes over a rating for all neighbors nodes in it wireless signal range. A Routeguard enhances Pathrather performance by distributing ratings to all participant nodes and measuring a path metric. Therefore, it demonstrates a more detailed and standard classification system that rates every node in the network.

Nasser and Chen [6] proposed an improved intrusion detection system for detecting malicious nodes in MANETs named ExWatchdog based on the Watchdog technique proposed by Marti et al. [3]. The researchers focus on the false misbehaving of the Watchdog technique, where a malicious node which is the actual intruder incorrectly reports another node as misbehaving. In ExWatchdog, a table is looked after by every node to record the quantity of packets the node forwards, receives or sends respectively. The source node will discover another path, when it obtains information of the misbehaving node, to enquire the destination node related to the number of received packets. The actual malicious node reports another node as misbehaving will be suspected, If the source node found that it is the same packets that it has sent. Otherwise, nodes being broadcasted information about a malicious node do false detection. However, there is still a drawback, it is impracticable to approve and confirm the number of packets with the destination node if the actual misbehaving node exists in all active paths from source to destination.

Parker et al in [7] proposed an improvement to an original the Watchdog technique which not only suitable for DSR protocol but also suitable to all routing protocols used in MANETs. In differentiating to the Watchdog, the nodes overhear all the other nodes in their neighborhoods and not only the next forward node on the path. The authors also proposed two response mechanisms, passive response and active response. The passive response mode performs freely, and eventually the intrusive node will be prevented from using all network resources. The second mechanism is the active response mode where the decision making is done by a cluster head which starting a voting procedure. If the majority decides that the suspected node is the intruder, and the intruder node will be prevented from using network resources. After all, an alert will be broadcasted throughout the network.

Animesh and Amitabh [8] proposed a method to improve performance of Watchdog technique by focus to the problem of collusion attack, which means a malicious

behavior from a collaboration of many nodes. The researchers assumed that the few nodes established the network are trusted nodes and the others that would join the network later are ordinary nodes. The Watchdog nodes are chosen from the trusted nodes to prevent the problem of inaccurate reporting. The two thresholds are maintained in every Watchdog, for all its neighbors that are not trusted nodes called SUSPECT_THRESHOLD and ACCEPTANCE_THRESHOLD respectively. The SUSPECT_THRESHOLD used for measure a node's misbehaving, and the ACCEPTANCE_THRESHOLD used for measure a node's good behavior. The Watchdog node will distinguish the neighboring nodes as a malicious or trusted node based on these thresholds.

Sonja Buchegger and Jean Boudec proposed another reputation mechanism called “CONFIDANT", which means for Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks [9]. The CONFIDANT has four main components, a reputation system, a monitor, a trust manager and a path manager. Each node implemented these components to monitor its neighbors by hearing to the transmission of the next node or by watching routing protocol behavior. A trust manager will be broadcasted alarm messages to all nodes in the network by when a misbehaving node is detected. The reputation system is used to measure nodes’ reputation in a network. A path manager is responsible to rank a path according to a security metric. Furthermore, a path manager will punish a selfish node by denying it all services. The simulation result of the performance of protocol in a scenario when a third of nodes behave selfishly showed that the throughput given by CONFIDANT is quite similar to the throughput of a usual network condition without selfish nodes. Since the CONFIDENT protocol relying on the Watchdog mechanism, it receives many of the Watchdog problems.

Michiardi et al. [10] proposed the other protocol that also uses a Watchdog mechanism called CORE, a COllaborative REputation mechanism. However, it is complemented by a complex reputation mechanism that differentiates from subjective reputation. This protocol includes of three main components, functional reputation, observations and indirect reputation that use positive reports by others. These three components are weighted for a combined reputation value that is used to take decisions about cooperation or gradual isolation of a node. Each node takes part in the IDS has reputation table and Watchdog mechanism. The reputation table keeps track of reputation values of other nodes in the network. Since a misbehaving node can accuse a good node, only positive rating factors can be distributed in CORE. This protocol also depends on the use of the Watchdog mechanism that inherited its disadvantages and problems.

3. Problem of routing misbehavior

In this section, we give elaborate more detail the problem caused by routing misbehavior. The design of routing protocols used in Wireless Ad Hoc networks such as DSR, AODV [21] and DSDV [22] are highly vulnerable to routing misbehavior due to faulty or compromised nodes. A selfish node operates normally in the Route Discovery and the Route Maintenance phases of the DSR protocol, but it does not intend to perform the packet forwarding function for data packets unrelated to it. The source node may being confused since such misbehaving nodes participate in the Route Discovery phase, they may be included in the routes chosen to forward the data packets from the source, but the misbehaving nodes refuse to forward the data packets from the source. In TCP, the source node may either choose an alternate route from its route cache or initiate a new Route Discovery process. The alternate route may again contain misbehaving nodes and the data transmission may fail again. However, the new Route Discovery phase will return a similar set of the same routes which including the misbehaving nodes. Eventually, the source node may conclude that routes are unavailable to deliver the data packets. This cause the network fails to provide reliable communication for the source node even though such routes are available. In UDP, the source simply sends out data packets to the next-hop node, which forwards them on. The existence of a misbehaving node on the route will cut off the data traffic flow. The source has no knowledge of this at all. Node’s misbehavior can be classified [11] into 3 categories as follow:

- Malfunctioning nodes: This behavior happen when nodes suffer from hardware failures or software errors.
- Selfish nodes: In this group, nodes refuse to forward or drop data packet and can be defined into three types [12] (i.e. SN1, SN2 and SN3). SN1 nodes take participation in the route discovery and route maintenance phases but refuse to forward data packets to save its resources. SN2 nodes neither participate in the route discovery phase nor in data-forwarding phase. Instead they use their resource only for transmissions of their own packets. SN3 nodes behave properly if its energy level lies between full energy-level E and certain threshold T1. They behave like node of type SN2 if an energy level lies between threshold T1 and another threshold T2 and if an energy level falls below T2, they behave like node of type SN1.
- Malicious: These nodes use their resource and aims to weaken other nodes or whole network by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control. After being selected in the requested route, they cause serious attacks either by dropping all received packets as in case of Black Hole attack [13], or selectively dropping packets in case of Gray Hole attack [14]. For convenience such malicious nodes are referred as MN nodes. SN2 type nodes do not pose significant threat therefore can simply be ignored by the routing protocol. On the other hand SN1, SN3 and MN nodes are much more dangerous to routing protocols. These nodes interrupt the data flow by either by dropping or refusing to forward the data packets thus forcing routing protocol to restart the route-discovery or to select an alternative route if it is available which in turn may again include some malicious nodes, therefore the new route will also fail. This process form a loop which enforce source to conclude that data cannot be further transferred.

4. Proposed Scheme

In this section, we elaborate more details of our solution to address the routing misbehavior. Our solution has two main processes. We detect the malicious activity in the first effort and then identify the malicious or compromised nodes in the network. Our scheme can be integrated on top of any source

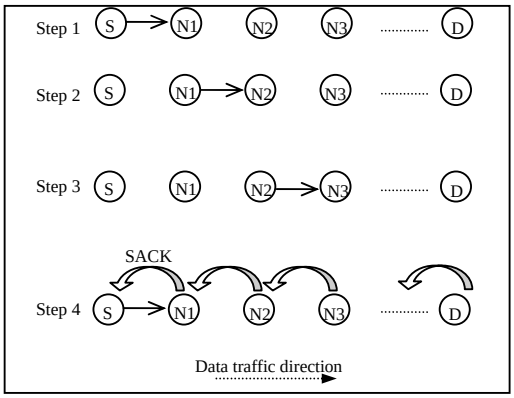

Fig.1 The SACK scheme

routing protocol such as DSR and AODV.

The Selective Acknowledgement (SACK) is a network layer acknowledgment-based scheme that considered as an enhancement system of an end-to end acknowledgment scheme (ACK). It aims to improve the performance of ACK scheme. It reduces the routing overhead of ACK while maintaining better performance and increases its detection efficiency by applying node detection instead of link detection. It is built on top of DSR routing protocol because it needs a source route protocol.

Figure 1 illustrates the operational detail of SACK scheme. Assume that the process of Routing Discovery has already established a source route from a source node S through N1,N2,N3 to a destination node D. In the SACK scheme, instead of sending back an acknowledge packets all the time when a data packet is received, a node wait until a curtain amount of data packets of the same source node arrive, then it send back one SACK packet acknowledge for multiple data packets that have been received. When a source node S send out any packet to a destination node D through its neighbor nodes N1, N2, N3, all these node add a packet ID in to a list of receive data packet as shown in figure 2. In stead of sending back an acknowledgement every time when a data packet is received, a node waits until a certain number of data packets of the same source node arrive. Then the node sends back one SACK packet acknowledging multiple data packets that have been received. If the source node receives a SACK packet from the destination that means there are no misbehaving nodes along the path.

Nid Neighbor ID	Mcount Misbehavior counter	ID_List List of data packet IDs Awaiting SACK

Fig.2. Data Structure of Misbehavior Detection List

Figure 2 illustrates the data structure of the Misbehavior Detection List. To detect misbehavior nodes, the sender of a data packet maintains a list of data packet IDs that receive a SACK packet from neighbor nodes. Each node maintains its unique list for each neighbor node. When a node, N1, sends or forwards a data packet to its neighbor node, N2, it adds the packet ID to its Misbehavior Detection List corresponding to N2. When it receives a SACK packet, it updates the node N2, and then removes the corresponding packet ID from the list. The node N2 will be suspected if its data packet ID stays on the list longer than a certain period of time, *time_out*. The misbehavior counter, *Mcount*, is increased by one when misbehavior is suspected. When *Mcount* reaches certain of threshold level, threshold, a node declares its neighbor node, N2, as a misbehaving node and broadcasts an RERR message to report a source node and all its neighbor nodes about this misbehavior node. All nodes in the same network update its misbehaving list and avoid this misbehaving node in the next routing process.

5. Conclusion

This paper presents a frame work in detecting misbehaving nodes and isolating such nodes from routing process in MANETs. This scheme can be combined on top of any source routing protocol such as DSR. A comprehensive analysis of routing misbehavior was made to develop a security module that would meet the network security goal. Currently we are working on its simulation in ns-2 simulator [15] to show the results and effectiveness of our solution on DSR routing protocol. Similar approaches can also be integrated to these source routing algorithms to address other attacks like black hole and gray hole attacks in MANETs.

Acknowledgement

We would like to thank Suan Dusit Rajabhat University and Universiti Teknologi Malaysia for supporting us.

References

[1] S. Alampalayam, A. Kumar, and S. Srinivasan, "Mobile ad hoc network security-a taxonomy," Advanced Communication Technology, ICACT 2005., pp. 839-844, 2005.
[2] F. Anjum and P. Mouchtaris, Security for Wireless Ad-hoc Networks: John Wiley & Sons, 2006.
[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), PP. 255-265, August 2000.
[4] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (dsr)," Published Online, IETF MANET Working Group, INTERNET-DRAFT, July 2004, expiration: January 2005. [Online]. Available: http://www.ietf.org/internetdrafts/draft-ietf-manet-dsr-10.txt
[5] Hasswa, A.; Zulkernine, M.; Hassanein, H., "Routeguard: an intrusion detection and response system for mobile ad-hoc networks," Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on , vol.3, no., pp. 336- 343 Vol. 3, 22-24 Aug. 2005

[6] Nasser, N.; Chen, Y., "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks,"Communications, 2007. ICC '07. IEEE
[7] Parker, J.; Undercoffer, J.; Pinkston, J.; Joshi, A., "On intrusion detection and response for mobile ad-hoc networks," Performance, Computing, and Communications, 2004 IEEE International Conference on , vol., no., pp. 747-752, 2004
[8] Patcha, A.; Mishra, A., "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," Radio and Wireless Conference, 2003. RAWCON '03. Proceedings, vol., no., pp. 75-78, 10-13 Aug. 2003
[9] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in MOBIHOC'02, 2002.
[10] P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in CMS'2002, Communication and Multimedia Security 2002 Conference, September 26-27, 2002.
[11] A. S. A. Ukey and M. Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET," IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010,pp. 12-17
[12] Abdelaziz Babakhouya, Yacine Challal, and Abdelmadjid Bouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks," in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008, pp. 592-597.
[13] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile Ad Hoc networks," in Proc. of the 42nd annual Southeast regional conference, ACM Southeast Regional Conference, April 2004, pp. 96–97.
[14] J. Sen, M.G. Chandra, S.G. Harihara, H. Reddy, and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," in Proc. of the 6th International Conference on Information, Communications & Signal Processing, December 2007, pp. 1-5.
[15] The Vint Project, "The ns-2 network simulator," http://www.isi.edu/nanam/ns
[16] C. E. Perkins, Ad-hoc Networking. Addison Wesley Professional,December 2000.
[17] M. Ilyas, ed., The Handbook of Ad-hoc Wireless Networks. CRC Press, December 2002.
[18] R. Hekmat, Ad-hoc Networks: Fundamental Properties and Network Topologies, Springer, 2006.
[19] M. Barbeau, E. Kranakis, Principles of Ad-hoc Networking. Wiley, 2007.
[20] S. K. Sarkar, T. G. Basavaraju, C. Puttamadappa, Ad Hoc Mobile Wireless Networks. Auerbach Publications, 2008.
[21] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug- 1998.
[22] C. Perkins, P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers",ACM SIGCOMM Computer Communication Review 1994; 24(4):234–244.

Nimitr Suanmali, is a Ph.D. student in the Dept. of Computer System and Communication, Faculty of Computer Science and Information System, University Teknologi Malaysia, Johor Bahru Malaysia. He received his B.Sc. degree in computer science from Suan Dusit Rajabhat University,Thailand in 1998, M.Sc. degree in Information Technology from King Mongkut's University of Technology Thonburi, Thailand in 2003. Since 2003, he has been working as lecturer at Suan Dusit Rajabhat University, Bangkok Thailand. His research interests include Network Security, Intrusion Detection and Intrusion Prevention, Wireless Ad-Hoc Networks, and Distributed Systems.

Kamalrulnizam bin Abu Bakar obtained his Ph.D degree in Computer Science (Network Security) from Aston University (Birmingham, UK) in 2004, B.S 1996 in Computer Science, Universiti Teknologi Malaysia and M.S. in Computer Communication & Networks, Leeds Metropolitan University, UK. in 1998. Currently, he is an Associate Professor in Computer Science at Universiti Teknologi Malaysia (Malaysia) and member of the "Pervasive Computing" research group. He involves in several research projects and is the referee for many scientific journals and conferences. His specialization includes mobile and wireless computing, information security and grid computing.

Suardinata, he is received the Diploma III 1999 in Information Management at AMIK Riau, Indonesia, Bachelor Degree in Information Engineering from STMIK Riau, Indonesia, and Master Degree in Information Technology from Universitas Putra Indonesia, Padang, Indonesia, Currently he is a Ph.D. student in the Dept. of Computer System and Communication, Faculty of Computer Science and Information System, University Teknologi Malaysia, Johor Bahru Malaysia. He has been working as Lecturer at STMIK Indonesia Padang from 2005 in the Dept. of Computer Science and Information Systems, STMIK Indonesia Padang. His research interests include Multimedia and Voice over IP network, Network Security, Traffic Engineering and Quality of Service issues in IP networks, Wireless Ad-Hoc Networks, and Distributed Systems.