Journal of Advances in Science and Technology

Vol. IV, No. VII, November-2012, ISSN 2230-9659

REVIEW ARTICLE

SECURE ROUTING TECHNIQUES IN MOBILE AD HOC NETWORK

www.ignited.in

Journal of Advances in Science and Technology
Vol. IV, No. VII, November-2012, ISSN 2230-9659

Secure Routing Techniques in Mobile Ad Hoc Network

Gundeep Tanwar

Research Scholar, CMJ University, Shillong, Meghalaya, India

---------------------------♦-----------------------------

INTRODUCTION

There are numerous kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks. In this part, we first discuss these two kinds of sophisticated attacks and then we introduce Watchdog and Pethrater which are two main components in a system that aims to mitigate the routing misbehaviors in mobile ad hoc networks. Finally we move to a secure ad hoc routing approach using localized self-healing communities.

DEFENSE METHOD AGAINST WORMHOLE ATTACKS IN MOBILE AD HOC NETWORKS

Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and replays them there into the network. The replay of the information will make great confusion to the routing issue in mobile ad hoc network because the nodes that get the replayed packets cannot distinguish it from the genuine routing packets. Moreover, for tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route, which makes the victim node be more likely to accept the tunneled packets instead of the genuine routing packets. As a result, the routing functionality in the mobile ad hoc network will be severely interfered by the wormhole attack. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication.

The notion of a packet leash as a general mechanism for detecting and, thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. There are two main leashes, which are geographical leashes and temporal leashes.A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows. A geographical leash in conjunction with a signature scheme (i.e., a signature providing nonrepudiation), can be used to catch the attackers that pretend to reside at multiple locations: when a legitimate node overhears the attacker claiming to be in different locations that would only be possible if the attacker could travel at a velocity above the maximum node velocity v, the legitimate node can use the signed locations to convince other legitimate nodes that the attacker is malicious [38].

The design of TIK protocol that implements the temporal leashes. The TIK protocol implements temporal leashes and provides efficient instant authentication for broadcast communication in wireless networks. TIK stands for TESLA with instant key disclosure, and is an extension of the TESL protocol. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio, or any other range that might be specified. The TIK protocol has been proved to be efficient since it requires just public keys in a network with nodes, and has relatively modest storage, per packet size, and computation overheads.

DEFENSE MECHANISM AGAINST RUSHING ATTACKS IN MOBILE AD HOC NETWORKS

Rushing attack is a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. This attack is also particularly damaging because it can be performed by a relatively weak attacker. The implementation details of rushing attacks are shown in the Figure .

In the network shown in Figure 3.4, the initiator node initiates a Route Discovery for the target node. If the

ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbor of the target (shown in gray in the figure), then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbor of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

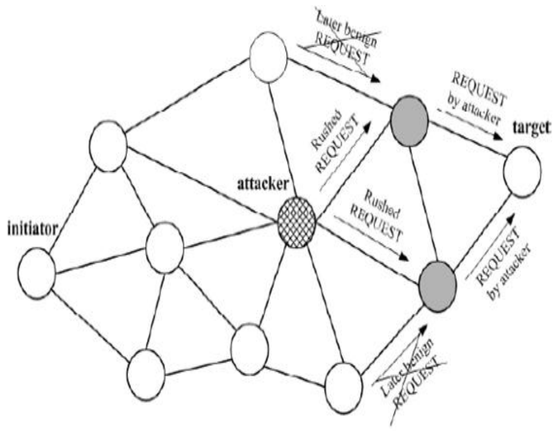

Figure 3.4: Rush Attack in the Example Ad Hoc Network

The rushing attack applies to all proposed on-demand protocols because such protocols must limit the number of packets that any node will transmit in response to a single Route Discovery. Currently proposed protocols choose to forward at most one REQUEST for each Discovery; any protocol that allows an attacker to predict which ROUTE REQUEST(s) will be chosen for forwarding at each hop will be vulnerable to some variant of the rushing attack.

A set of generic mechanisms that together defend against the rushing attack: secure Neighbor Detection, secure route delegation, and randomized ROUTE REQUEST forwarding. The relations among these security mechanisms are shown in Figure 3.5.

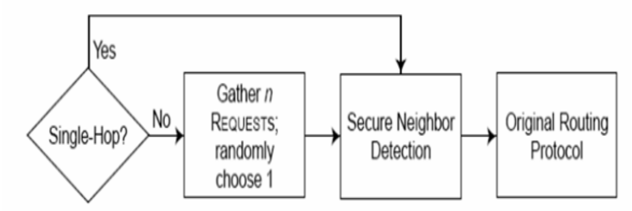
Yes
Single-Hop?
No
Gather n REQUESTS; randomly choose 1
Secure Neighbor Detection
Original Routing Protocol

Figure 3.5: Combined Mechanisms to Secure MANET against Rushing Attacks

Secure Neighbor Detection allows each neighbor to verify that the other is within a given maximum transmission range. Once a node A forwarding a ROUTE REQUEST determines that node B is a neighbor (that is, is within the allowable range), it signs a Route Delegation message, allowing node B to forward the ROUTE REQUEST. When node B determines that node A is within the allowable range, it signs an Accept Delegation message. In this way, the neighborhood relationships between nodes can be verified and guaranteed to be genuine.

Randomized selection of the ROUTE REQUEST message to forward, which replaces traditional duplicate suppression in on-demand route discovery, ensures that paths that forward REQUESTs with low latency are only slightly more likely to be selected than other paths, but not guaranteed to be selected.

A protocol to protect the ad hoc networks from rush attacks, which is called Rushing Attack Prevention (RAP). When integrated with a secure routing protocol, RAP incurs no cost unless the underlying secure protocol cannot find valid routes. When RAP is enabled, it incurs higher overhead than do standard Route Discovery techniques, but it can find usable routes when other protocols cannot, thus allowing successful routing and packet delivery when other protocols may fail entirely.

WATCHDOG AND PATHRATER

Watchdog and Pathrater are two main components of a system that tries to improve performance of ad hoc networks in the presence of disruptive nodes, the specific working principles of which are discussed below:

Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped match with the observing node’s buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious. Information about malicious nodes is passed to the Pathrater component for inclusion in path rating evaluation.

Pathrater on an individual node works to rate all of the known nodes in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular node’s perspective. Nodes start with a neutral rating that is modified over time based on observed reliable or unreliable behavior during packet routing. Nodes that are observed by watchdog to have misbehaved are given an immediate rating of -100. It should be distinguished that misbehavior is detected as packet mishandling/modification, whereas unreliable behavior is detected as link breaks.

A SECURE AD HOC ROUTING APPROACH USING LOCALIZED SELF-HEALING COMMUNITIES

Two routing attacks that use non-cooperative network members and disguised packet losses to deplete ad hoc network resources and to reduce ad hoc routing performance, which are called RREQ resource depletion and RREP packet and data packet loss, respectively.

In the RREQ resource depletion attack, an attacker sends RREQ packets, which the underlying on-demand routing protocol floods throughout the network. If the attacker is not a network member, cryptographic authentication can be added to RREQ packets to filter out those forged route discovery requests. However, if the attacker is a compromised or selfish network member, the cryptographic countermeasures are ineffective. In the RREP packet and data packet loss attack, when a route discovery procedure is initiated by a good network member, an attacker can use “wormhole attack” or “rushing attack” to surpass other nodes with respect to the underlying routing metric. Then it is highly likely the attacker is selected en route. When the RREP comes back it may not forward or may forward a corrupted one. The result is equivalent to RREQ resource depletion attack, except now the RREQ initiator is not the one to blame. Also an attacker can severely degrade data delivery performance by selectively dropping data packets.

Next we briefly discuss the concept of “self-healing community” and its application in the secure ad hoc routing. The concept of “self-healing community” is based on the observation that wireless packet forwarding typically relies on more than one immediate neighbor to relay packets. Community-based security explores node redundancy at each forwarding step so that the conventional per-node based forwarding scheme is seamlessly converted to a new percommunity based forwarding scheme. Since a self-healing community is functional as long as there is at least one cooperative “good” node in the community, there is no requirement that how many nodes in the community should be available to provide reliable packet forwarding services [39]. There are one configuration and one reconfiguration protocol that can respectively be used to initially set up the self-healing community and fix the community if there is a shape loss due to the mobility or change of topology.

REFERENCES

[1] Wang, Weichao, L Yi, Bharat Bhargava. On Vulnerability and protection of Ad hoc On Demand Distance Vector Protocol.

http://www.cs.purdue.edu/homes/wangwc/ICT03wangwc.pdf

[2] Jakobsson, Markus; Wetzel, Susanne and Yener, Bulent. Steal Attack on Adhoc Wireless Networks.

http://Guinness.cs.steven.edu/~swetzel/papers/stealth.pdf

[3] Martin, Frederic; Thao, Houy-Sy; Thylander, Magnus. Security in Ad-hoc Routing Protocols.

http://www.comp.nus.edu.sg/~cs4274/tempapers/0304-I/group1/present.ppt

[4] Mishra, Amitabh; Nadkarni, Ketan M.; Ilyas, Mohammad, editor. Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network. CRC PRESS Publisher, 2003.

[5] Murthy, C. Siva Ram, Manoj, B. S; Ad hoc Wireless Networks: Architectures and Protocols. Prentice Hall.

http://www.parc.com/zhao/stanford-cs428/readings/Networking/Royer_IEEE_Personal_Comm99.pdf

[6] Hu, Yih-Chun; Johnson, David B.; Perrig, Adrian. ARIADNE: A Secure On-Demand Routing Protocol for Ad hoc Networks.

http://www.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf

[7] OPNET Modeler 11.0 Documentation: API Reference Manuals.

[8] Zapata, Manel Guerrero. Secure Ad hoc On-Demand Distance Vector Routing.

http://www.cse.cuhk.edu.hk

[9] Sadasivam, Karthik; Vishal, Changrani; T. Andrew Yang: Scenario Based Performance Evaluation of Secure Routing in MANETs

http://sce.uhcl.edu/sadasivamk/MANETII05-draft.pdf

[10] Ad hoc routing protocol list.

http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols.

Last accessed March 2007.

[11] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET on demand (DYMO) routing protocol. Internet-Draft Version 06, IETF, October 2006, (Work in Progress).

[12] Ian D. Chakeres and Elizabeth M. Belding-Royer. The utility of hello messages for determining link connectivity. In Proceedings of the 5th International Symposium of Wireless Personal Multimedia Communications (WPMC) 2002, volume 2, pages 504–508, Honolulu, Hawaii, October 2002

[13] Sumit Gwalani, Elizabeth M. Belding-Royer, and Charles E. Perkins. AODV-PA: AODV with path accumulation. In IEEE International Conference on Communications (ICC' 03), volume 1, pages 527–531, Anchorage, Alaska, May 2003. IEEE.

[14] Elizabeth Belding-Royer, Ian Chakeres, David Johnson, and Charlie Perkins. DYMO – dynamic MANET on-demand routing protocol. In Rebecca Bunch, editor, Proceedings of the Sixty-First Internet Engineering Task Force, Washington, DC, USA, November 2004. IETF.

[15] S.A. Razak, S.M. Furnell, N.L. Clarke, and P.J. Brooke, "Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks," Ad Hoc Networks,vol. In Press, Corrected Proof.

[16] A.P. Lauf, R.A. Peters, and W.H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," Ad Hoc Networks, vol. In Press, Corrected Proof, 2009.

[17] N. Marchang, and R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," Ad Hoc Networks, vol. In Press, Corrected Proof