Research Findings on Wormhole Attack Detection in Mobile Ad Hoc Networks

Conference or Workshop Item

Research Findings on Wormhole Attack Detection in Mobile Ad Hoc Networks

Jonny Karlsson[1, 2], Laurence S. Dooley[2] and Göran Pulkkis[1]

Abstract

The Internet is moving from the traditional desktop network paradigm to a ubiquitous paradigm where a multitude of small computing devices such as computer chips and smart sensors are involved in daily activities and routines. This means that a rapidly growing amount of devices are connected to the Internet. At the same time, infrastructure-less and self-configuring systems like Mobile Ad hoc Networks (MANET) are gaining popularity since they provide a possibility for mobile devices to share information with each other without being dependent on a core infrastructure. Routing security in MANETs is, however, a significant challenge to wide scale adoption. One of the most severe security threats to MANET routing is the wormhole attack due to its ability to disrupt a significant proportion of network traffic, while simultaneously being difficult to detect. This paper provides an overview of recent research findings on wormhole attack detection in MANETs collected from a joint research project with Arcada University of Applied Sciences in Finland and The Open University, UK.

1. Introduction

A Mobile Ad hoc Network (MANET) is a self-configuring arrangement of mobile devices interconnected by wireless links, with no fixed infrastructure like base stations and dedicated routers. Examples of MANET implementations are wireless sensor networks, vehicular networks, military communication networks, and Internet connectivity networks where some of the nodes are located out of the radio range of an Internet connection point, as for example in underground transport systems.

Due to their self-configuring nature, each MANET node participates in the routing process, in addition to its other activities. Several routing protocols have been proposed for MANETs, such as Ad Hoc On Demand Distance Vector (AODV) (Perkins & Royer 1999) and Dynamic Source Routing (DSR) (Johnson & Maltz 1996), but security has typically not been a priority in routing protocol development. In a large scale MANET integrated in the future world of an 'Internet of Things' (IoT) where lots of devices dynamically enter and leave the network, it is difficult to establish trust relationships among nodes. Therefore, routing in a MANET is especially vulnerable to malicious node activities leading to a potentially severe disruption in network communications (Karlsson, Dooley & Pulkkis 2012, Agrawal, Jain & Sharma 2011). Such disruption can range from deliberately ignoring the routing protocol, through to tampering with routing packets. For example, to save energy a selfish node may simply not take part in the routing process, leading to packet loss. A malicious node however, can launch serious network attacks such as rerouting packets from their original path to an erroneous destination node or even stealing the identity of another node.

1 Arcada University of Applied Sciences

2 The Open University, Milton Keynes, United Kingdom

The wormhole attack (Hu, Perrig & Johnson 2003) is one of the most severe MANET routing threats since it is easy to launch, difficult to detect and can cause significant communication disruption. Two collaborating malicious nodes create a fictive shortcut link in the network by forwarding routing packets to each other with the intention of attracting more data packets to traverse the wormhole link. Once the wormhole has been successfully established, the malicious nodes can disrupt network operation by either dropping packets or launching more serious attacks, such as eavesdropping and packet sniffing.

A wormhole attack can be launched in either hidden mode (HM) or participation mode (PM) (Khabbazian, Mercier & Bhargava 2006). In the former, malicious nodes capture and forward routing packets to each other without modifying the actual packets, so the wormhole nodes never appear in routing tables. In contrast, PM nodes process routing packets as any pair of legitimate nodes and then appear in a wormhole infected route as two contiguous nodes.

The malicious nodes can forward routing packets to each other using either an in-band (I-B) or out-of-band (O-B) wormhole link. I-B links tunnel packets between the malicious nodes via genuine network nodes and are therefore easy to launch, while the O-B link is more complex because it requires an external communication channel, i.e., network cable or directional antenna, to establish a direct link between the wormhole nodes.

Various wormhole detection strategies have been proposed (e.g. Hu, Perrig & Johnson 2003, Khabbazian, Mercier & Bhargava 2009, Song, Wu & Choi 2012, Khurana & Gupta 2008), but most solutions have some recurring limitations including the inability to detect all wormhole types, the requirement for dedicated hardware, a reliance on particular MANET environments, and imposing high computational overheads and/or bandwidth loads upon the network.

This provided the motivation to design and analyse a new wormhole detection scheme called Traversal Time and Hop Count Analysis (TTHCA) (Karlsson, Dooley & Pulkkis 2011) which is designed as a security extension to the AODV (Perkins & Royer 1999) routing protocol. It combines the benefits of Round Trip Time (RTT)-based approaches such as Wormhole Attack Prevention (WAP) (Choi et al. 2008), Transmission Time-based Mechanism (TTM) (Tran et al. 2007) and Delay Per Hop Indication (DelPHI) (Chiu & Lui 2006) with Multi Hop count Analysis (MHA) (Jen, Laih & Kuo 2009), to provide improved detection for several wormhole attack conditions and in a wide range of network scenarios.

RTT based approaches offer low overhead solutions in terms of hardware, computation and throughput, but have the limitation that variations in a node's packet processing time, must be small. In a real MANET, nodes can exhibit high packet processing time variations resulting in that a route with only a few hops can often have a higher RTT than a route with many hops. MHA on the other hand relies on a wormhole infected route always having a significantly lower Hop Count (HC) compared to a healthy route which has been proven to be false through simulations.

2. Traversal Time and Hop Count Analysis (TTHCA)

The original idea of TTHCA (Karlsson, Dooley & Pulkkis 2011) is to let a source node estimate the PTT of a routing packet instead of the RTT, since the PTT is close to constant for a certain distance whilst RTT can vary due to fluctuations in queuing delay at intermediate nodes. In TTHCA, PTT is calculated by first letting the source node measure the RTT of the AODV route discovery packets, which is the time between sending the RREQ packet and receiving the RREP packet. Each intermediate node measures the processing time of the RREQ and RREP packets and this value (ΔTi) is added to a new parameter of the RREP packet. Hence, once an RREP packet is received by the source node, the source can estimate PTT by simply reducing the sum of all ΔTi from the RTT. Finally, a wormhole is suspected if the PTT in relation to the route HC is unrealistically high.

2.1 Preventing Time Tampering in TTHCA

Malicious wormhole nodes can, however, potentially prevent TTHCA from detecting infected routes by adding a fictive packet processing time value parameter to the RREP packet. Such a time tampering attack is not a modification attack, as the wormhole node never alters any routing packet parameters, but instead produces false measurement information. This means that schemes designed to prevent packet alteration by, for example, encrypting all routing packet parameters, will be ineffectual against a TTHCA time tampering attack. So, a malicious node can prevent the wormhole from being detected if

it presents a higher ΔTi than the actual packet processing time. By increasing ΔTi the source node will calculate a smaller PTT/HC and therefore the wormhole can potentially go undetected. However, from the attackers' point of view, time tampering is not a trivial task since it has to increase the ΔTi within a strict time window which is difficult for the attacker to be aware of. For example, if a malicious node provides a ΔTi that is too high, the source node will calculate a negative PTT/HC. If however the malicious nodes are aware of the exact delay of the wormhole link (which is technically possible), a successful time tampering attack is conceivable.

To minimize this threat we have proposed an extension to TTHCA requiring each intermediate node to store its ΔTi in a separate element of a new ΔTi Vector parameter of the RREP packet. As a result, when receiving the RREP, the source node can apply a statistical outlier detection mechanism for checking the validity of each ΔTi in the vector. If one or more of the ΔTi values are statistically significantly higher than the average, a time tampering attack is suspected and the route is omitted.

The time tampering problem, an analysis of its impacts on TTHCA wormhole detection performance, and the ΔT Vector extension is presented in detail by (Karlsson, Dooley & Pulkkis 2013).

3. Performance analysis

The performance of both TTHCA and the ΔT Vector extension has been rigorously tested through simulation. This section provides an extract of the simulation results previously published (Karlsson, Dooley & Pulkkis 2011; 2013).

3.1 TTHCA Wormhole Detection

TTHCA was tested and compared with MHA (Jen, Laih & Kuo 2009) and DelPHI (Chiu & Lui 2006) in a MANET simulation environment developed in NS-2 (The Network Simulator 2013). The environment consisted of 300 nodes with identical hardware, and random node placements for each simulation run. The network was infected by a single wormhole with different lengths. The simulations showed that TTHCA can detect all wormholes in the simulation environment, either when the wormhole is launched in HM and/or using an I-B channel.

A PM O-B wormhole is the most challenging to detect for TTHCA and RTT-based wormhole detection schemes since the malicious nodes tunnel packets through each other over a low delay communication link, for instance by using a directional antenna or network cable. The simulation results revealed that TTHCA still provides significantly improved wormhole detection performance compared to both MHA and DelPHI, see Figure. 1.

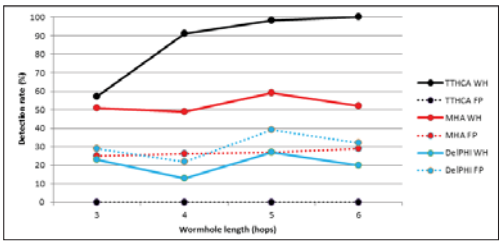

Figure 1. PM O-B wormhole (WH) detection and false positive (FP) occurrence performance (Karlsson, Dooley & Pulkkis 2011)

3.2 Time Tampering Detection Performance of the Δ-T Vector Mechanism

Time tampering detection performance was simulated with the underlying assumption that each wormhole node was always aware of the required time tampering windows, meaning that they were able to prevent every wormhole from being detected by the original TTHCA algorithm. A custom tool was developed to generate different ΔTi values for traffic loads and packet service times at the nodes. Dixon Q-test (Dean &Dixon 1951) was applied for identifying tampered ΔTi values. The time tampering detection performance assumed the source node had a track record of at least 15 earlier measured ΔTi values and the MANET was infected by a PM I-B wormhole, is shown in Figure 2. Different wormhole lengths and variability in both node traffic load and packet service time were tested.

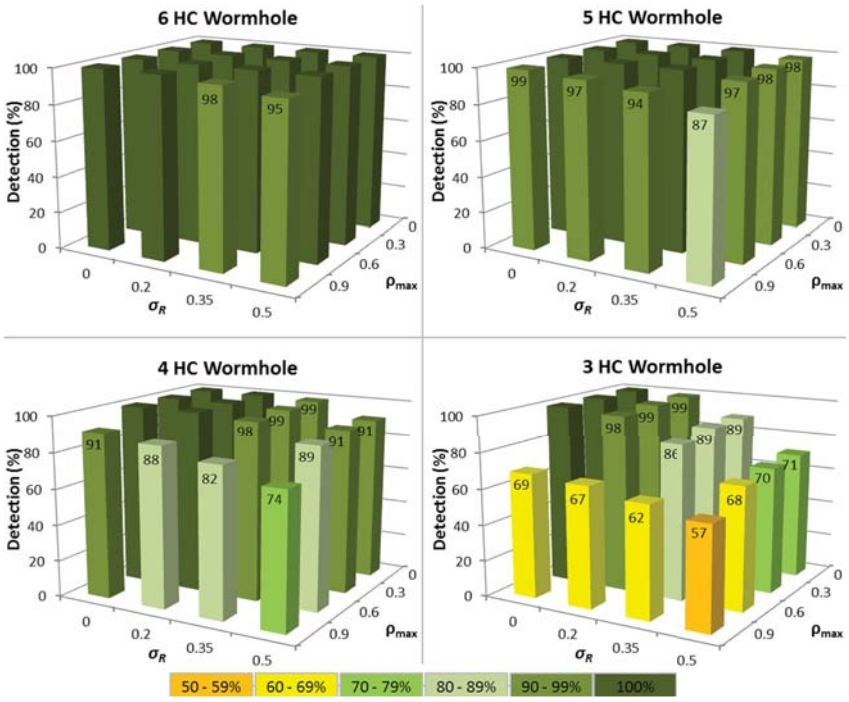

Figure 2. Time tampering detection performance for different wormhole hop count (HC) for variable network traffic loads (max) and routing packet service times (R) (Karlsson, Dooley & Pulkkis 2013)

4. Conclusions and future research

Wormhole attacks are one of the most severe threats to MANET routing and are difficult to detect as they can be launched in several modes, each enforcing its own distinct requirements on the detection mechanism employed. Most wormhole attack detection schemes presented in the literature have limitations, such as a lack of ability to detect all wormhole types, the requirement for additional hardware such as GPS, or a requirement for a certain network condition in order to be effective. We have proposed a wormhole detection algorithm called Traversal Time and Hop Count Analysis (TTHCA) which by way of simulations has been proven to be effective on all types of wormholes and in a wide range of network conditions, incurring neither significant computational nor network costs.

We have also identified a limitation of TTHCA which is the possibility for malicious nodes to tamper with the packet processing time measurements and hence potentially prevent the wormhole from being detected. The conditions for a time tampering attack have been thoroughly analysed and a new security mechanism called the ΔT Vector extension has been proposed for detecting false time values.

In terms of future research, an important aim for the TTHCA algorithm is to make the threshold used for defining the maximum allowed packet traversal time per hop count, adaptive to its surroundings. TTHCA among many other proposed wormhole detection solutions assumes constant radio ranges which does not reflect a real world scenario that consists of a variable set of obstacles (such as walls) between MANET nodes and different hardware, both causing a variability in radio ranges. Therefore, the need is to generate a threshold for TTHCA that can adapt to both its surroundings and also to a rapid change of environment such as moving from outdoors to indoors, since such a situation can momentarily cause a significant decrease of wormhole detection performance.

An experimental network is also planned for testing the time measurement accuracy on different hardware and the propagation speed of wireless signals in different environments, factors which are important for making TTHCA applicable in a real MANET implementation.

REFERENCES

AGRAWAL, S., Jain, S. & Sharma, S. 2011, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks." Journal of Computing, Vol. 3, pp. 41-48.

AZER, M.A., El-Kassas, S.M. & El-Soudani, M.S. 2009, "Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks." In: Fourth International Conference on Systems and Networks Communications (ICSNC '09), Porto, Portugal.

CHIU H. S. & Lui K-S. 2006, "DelPHI: Wormhole Detection Mechanism for Ad hoc Wireless Networks", In: 1st International Symposium on Wireless Pervasive Computing (ISWPC'16), Phuket, Thailand.

CHOI, S., Kim, D-Y., Lee, D-H. & Jung, J-I. 2008, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks." In: International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC '08), Taichung, Taiwan.

DEAN, R.B. & Dixon, W.J. 1951, "Simplified Statistics for Small Numbers of Observations." Analytical Chemistry, Vol. 23, nr 4, pp. 636-638.

HU, Y., Perrig, A. & Johnson, D.B. 2003, "Packet leashes: a defense against wormhole attacks in wireless networks." In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM'03). San Fransico, CA, USA.

JEN, S., Laih, C. & Kuo, W. 2009, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET." Sensors, Vol. 9, nr 6, pp. 5022-5039.

JOHNSON, D.B. & Maltz, D.A. 1996, "Dynamic Source Routing in Ad Hoc Wireless Networks." Mobile Computing, Vol. 353, pp. 153-181.

KARLSSON, J., Dooley, L. S. & Pulkkis, G. 2012, "Routing Security in Mobile Ad-hoc Networks." Issues in Informing Science & Information, Vol. 9, pp. 369-383

KARLSSON, J., Dooley, L.S. & Pulkkis, G. 2013, "Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm." Sensors, Vol. 13, nr 5, pp. 6651-6668.

KARLSSON, J., Dooley, L.S. & Pulkkis, G. 2011, "A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis." Sensors, Vol. 11, nr 12, pp. 11122-11140.

KHABBAZIAN, M., Mercier, H. & Bhargava, V.K. 2009, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks." IEEE Transactions on Wireless Communications, Vol. 8, nr 2, pp. 736-745.

KHABBAZIAN, M., Mercier, H. & Bhargava, V.K. 2006, "NIS02-1: Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure. " In: Global Telecommunications Conference (GLOBECOM '06), San Francisco, CA, USA.

KHURANA, S. & Gupta, N. 2008, "FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks." In: Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '08), Cap Esterel, France.

PERKINS, C.E. & Royer, E.M. 1999, "Ad-hoc on-demand distance vector routing."In: Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99), New Orleans, LA, USA.

QIAN, L., Song, N. & Li, X. 2005, "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path." In: Wireless Communications and Networking Conference (WCNC'05), New Orleans, LA, USA.

SONG, S., Wu, H. & Choi, B. Y. 2012, "Statistical wormhole detection for mobile sensor networks", In: Fourth International Conference on Ubiquitous and Future Networks (ICUFN'12), Phuket, Thailand.

SU, M. 2010, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks." Computers & Security, Vol. 29, nr 2, pp. 208-224.

THE Network Simulator - ns-2 2013, Available: http://www.isi.edu/nsnam/ns/ Retrieved October 14, 2013.

TRAN, P.V., Hung, L.X., Lee, Y., Lee, S. & Lee, H. 2007, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks." In: 4th IEEE Consumer Communications and Networking Conference (CCNC 2007), Las Vegas, NV, USA.