A Survey Article on Wormhole Attack Detection and Security in Wireless Sensor Networks

Harpal
Research Scholar,
Shri Venkateshwara
University,Gajraula, India

Gaurav Tejpal,PhD
Professor,
Shri Venkateshwara University
Gajraula, India

Sonal Sharma,PhD
Assistant Professor,
Uttaranchal University
Dehradun, India

ABSTRACT

For the duration of multihop portable methods, including ad-hoc and also indicator / probe sites, the prerequisite for co-operation amongst nodes in order to trade one another's offers shows the crooks to numerous security attacks. A particularly damaging attack is called your wormhole attack, where the harmful node documents command and also data traffic at 1 place and also routes that to the colluding node, which replays that locally. This could have a damaging result about Class Company by simply defending against nodes through obtaining tracks which will are far more than 2 trips away. During this paper, we active a light countermeasure for the wormhole attack, known as LITEWORP, which does not involve specific hardware. LITEWORP is quite suitable for resource-constrained multihop portable sites, including indicator / probe networks. Our own selection permits finding of one's wormhole, with rural location of one's harmful nodes. Simulators ultimate effects demonstrate that pretty much every wormhole is available and also remote in very a quick time period greater than a huge selection of scenarios. The final effects also demonstrate your portion with offers missing consequently of wormhole as soon as LITEWORP is used is negligible than the reduction encountered as soon as the tactic is just not applied.

Keywords

Wormhole Attack, Security, Wireless Ad-hoc Networks.

1. INTRODUCTION

In a wormhole attack, wireless signals are noted at one location and replayed at yet another, producing a digital link under opponent control. Planned counter-measures to the attack use limited time synchronization, particular electronics, or overhearing, making them hard to realize in practice. True Link is a moment centered countermeasure to the wormhole attack. Using True Link, a node i can confirm the living of a direct url to an apparent neighbor, j. Evidence of a link i harr j runs in two phases. In the rendezvous period, the nodes change nonce's alpha$_i$ and beta$_j$. That is completed with limited moment constraints, within which it is impossible for opponents to forward the change between remote nodes. In the certification period, i and j send closed information (alpha$_i$, beta$_j$), mutually authenticating themselves while the designer of their respective nonce. True Link doesn't count on precise time synchronization, GPS coordinates, overhearing, geometric inconsistencies, or mathematical methods. It could be implemented using just standard IEEE 802.11 electronics with a backwards appropriate firmware update. True Link is meant to be used together with a secure routing protocol. Such practices involve an certification mechanism, which may also be utilized by True Link. True Link is virtually separate of the routing protocol used. Our efficiency evaluation demonstrates True Link provides successful defense against potentially destructive wormhole attacks. Wireless offer hoc communities are imagined to be arbitrarily deployed in functional and potentially hostile environments. Thus, giving protected and uninterrupted communication between the un-tethered network nodes becomes a vital problem. In that report, we examine the wormhole attack in wireless offer hoc communities, an attack that can affect vital network functions such as for example routing. In the wormhole attack, the adversary establishes a low-latency unidirectional or bi-directional link, such as a wired or long-range wireless link, between two points in the network which are not within communication selection of every other. The opponent then files more than one communications at one conclusion of the hyperlink, tunnels them via the hyperlink to one other conclusion, and replays them to the network in a timely manner. The wormhole attack is simply implemented and specially challenging to find, since it does not involve breach of the credibility and confidentiality of communication, or the compromise of any host. We provide a graph theoretic platform for modeling wormhole hyperlinks and gain the required and adequate situations for detecting and defending against wormhole attacks. Centered on our platform, we reveal that any candidate option avoiding wormholes must develop a communication graph that's a sub graph of the geometric graph explained by the air selection of the network nodes. Utilizing our platform, we propose a cryptographic mechanism centered on *regional transmitted secrets* to be able to prevent wormholes. Our option does not want time synchronization or time rating, needs just a small fraction of the nodes to learn their location, and is decentralized. Thus, it is ideal for communities with the most stringent constraints such as for example alarm networks. Eventually, we feel our perform is the first ever to give an analytic evaluation in terms of probabilities of the level to which a way prevents wormholes.

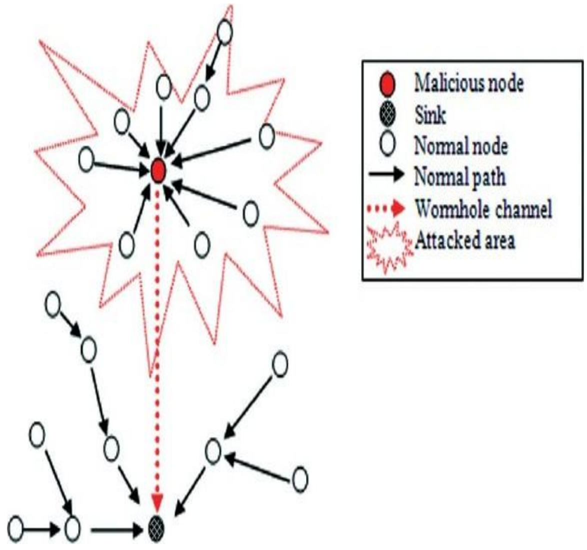

Fig 1: Wormhole attack detection path

2. SECURITY ISSUES FOR WORMHOLE ATTACK

In an offer hoc system, many scientists have labored on pretending and detecting wormhole problems specifically. In part A we discuss a technique named ‘box leads ', which allows avoiding packages from touring further than radio sign range. In part B explain about wormhole elimination practices that rely on Circular Journey meaning Time (RTT). Ultimately, in part D we discuss wormhole recognition or elimination practices suitable for just specific kinds of sites and in N discuss summary of wormhole finding methods.

2.1 Packet leads

Packet Lead in[5/6/7] is really a mechanism to find and defend against wormhole attacks. The mechanism proposes two types of leads for this function: Geographic and Temporal. In Geographic Leashes, each node knows their accurate place and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends their current place and transmission time and energy to it. The obtaining node, on bill of the box, computes the exact distance to the sender and the full time it took the box to traverse the path. The receiver may make use of this distance anytime data to deduce whether the obtained box passed by way of a wormhole or not. In Temporal Leashes, all nodes are needed to keep up a tightly synchronized time but don't depend on GPS information.

2.2 Time-of-flight

Yet another pair of wormhole reduction practices is similar to temporal box leads in [6], is on the basis of the time of journey of individual packets. One possible way to prevent wormholes, as utilized by Capkun et al in [9] is to measure round-trip travel time of a note and their acknowledgement, estimate the exact distance involving the nodes based on this travel time, and establishes whether the calculated distance is within the maximum possible communication range. However, note that wormhole opponents are not confined by the guidelines of the system, and can send their boxes without 802.11-imposed delay. Approaches predicated on RTT that one node sends a packet to a different, the clear answer should arrive very fleetingly, preferably within the amount of time a wireless signal could travel involving the nodes. If you have a wormhole opponent included, boxes find yourself World Academy of Technology, Design and Technology 24 2008 423 traveling farther, and thus can not be returned inside a small time.

2.3 Specialized Practices

A wide selection of wormhole strike mitigation practices have now been planned for unique kinds of networks: warning networks, fixed networks, or networks wherever nodes use online antennas. In that section, we explain and examine such practices, commenting on their usability and the likelihood of these use in standard mobile MANETs. Hu and vans propose a remedy to wormhole attacks for advertising hoc networks where all nodes are equipped with online antennas in [10]. In that process nodes use unique ‘areas ‘of these antennas to keep in touch with each other. Each couple of nodes needs to examine the direction of obtained signs from its neighbour. Thus, the neighbour connection is set as long as the guidelines of both pairs match. That added little bit of data makes wormhole discovery and presents substantial inconsistencies in the system, and can very quickly be detected. Wang and Bhargava [11] add an method where system visualization is used for discovery of wormhole attacks in fixed warning networks. In their method, each warning estimates the exact distance to its neighbours utilising the obtained indicate strength. All receptors deliver that distance data to the central controller, which determines the network's bodily topology centered on specific warning distance measurements. With no wormholes provide, the system topology must be pretty much flat, while a wormhole would be viewed as a ‘sequence’ dragging different stops of the system together. Lazos et al [12] planned a ‘graph-theoretical ‘way of wormhole strike elimination based on the use of Location Aware ‘Protect ‘Nodes (LAGNs). Lazos uses ‘regional broadcast tips'- tips valid only between one-hop neighbours - to defy wormhole opponents: an email secured with a nearby essential at one conclusion of the system can't be decrypted at yet another end. Khalil et al [2] propose a project for wormhole strike discovery in fixed networks they call LiteWorp. In LiteWorp, after stationed, nodes acquire complete two-hop routing data from their neighbours. During a standard advertising hoc routing project nodes frequently keep track of their neighbours are, in LiteWorp additionally they know who the neighbour- neighbour are, - they can make the most of two-hop, rather than one-hop, neighbour information. These records can be exploited to identify wormhole attacks. Also, nodes observe their neighbours' behavior to determine whether knowledge packets are now being precisely forwarder by the neighbour.

3. TECHNIQUES FOR WORMHOLE DETECTION

There are many simple practices to discover wormholes in a network but these have some basic imperfections which are discussed in following section.

3.1 Url Volume Analysis

Analysis of the web link volume is just a simple solution to discover a wormhole in a network. Extraordinarily high volume of a url can suggest so it can be quite a wormhole luring traffic into it. But in the case of cluster networks where in actuality the bottleneck hyperlinks present similar delays as that of a wormhole in the network, the traffic could be equally spread involving the bottleneck url and the wormhole url and there's no way to get whether there's a wormhole and if discovered, it will soon be hard to recognize the wormhole link.

3.2 Confidence Based Model

Still another substantial solution to discover wormholes is by the use of confidence information. Nodes can monitor the behaviour of the neighbour and rate them. Accepting that a wormhole falls all of the packets it gets as in blackholes, a wormhole in such a system should have the smallest amount of confidence stage and could be simply eliminated. Drops in bottleneck in a network might be as a result of obstruction, which may be brought about by incorrect routing, high TCP window dimensions, and quick breaks of traffic from a node etc. But all these falls occur in breaks and network gets reconfigured after congestion. As an example, if there are a large amount of falls in TCP, the window size is decreased. Ergo, the drop of packets in bottleneck is generally high just throughout obstruction after which it is produced down again.

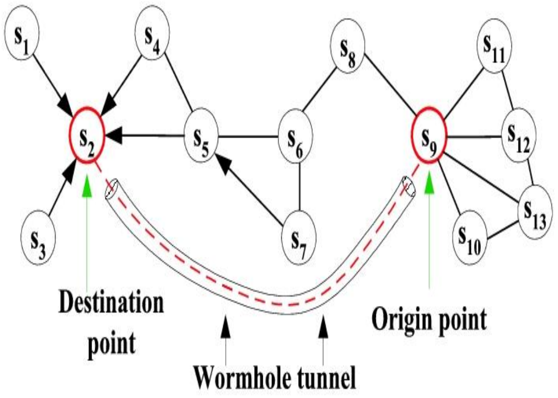

Fig 2: Wormhole Detection

4. CONCLUSION

During this paper, we active a light countermeasure for the wormhole attack, known as LITEWORP, which does not involve specific hardware. LITEWORP is quite suitable for resource-constrained multihop portable sites, including indicator / probe networks. Our own selection permits finding of one's wormhole, with rural location of one's harmful nodes. Simulators ultimate effects demonstrate that pretty much every wormhole is available and also remote in very a quick time period greater than a huge selection of scenarios. The final effects also demonstrate your portion with offers missing consequently of wormhole as soon as LITEWORP is used is negligible than the reduction encountered as soon as the tactic is just not applied. In future different techniques can be used to detect and prevent wormhole attack like bee colony optimization, clustering, fuzzy logic etc.

5. REFERENCES

[1] Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks." Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on. IEEE, 2005.

[2] Eriksson, Jakob, Srikanth V. Krishnamurthy, and Michalis Faloutsos. "Truelink: A practical countermeasure to the wormhole attack in wireless networks." Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference on. IEEE, 2006.

[3] Choi, Sun, et al. "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks." Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on. IEEE, 2008.

[4] Poovendran, Radha, and Loukas Lazos. "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks." Wireless Networks 13.1 (2007): 27-59.

[5] Wang, Xia, and Johnny Wong. "An end-to-end detection of wormhole attack in wireless ad-hoc networks." Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International. Vol. 1. IEEE, 2007.

[6] Win, Khin Sandar. "Analysis of detecting wormhole attack in wireless networks." World Academy of Science, Engineering and Technology. 2008.

[7] Jhaveri, Rutvij H., et al. "MANET routing protocols and wormhole attack against AODV." International Journal of Computer Science and Network Security 10.4 (2010): 12-18.

[8] Jain, Mohit, and Himanshu Kandwal. "A survey on complex wormhole attack in wireless ad hoc networks." Proceedings of International Conference on Advances in Computing, Control, and Telecommunication Technologies (ACT'09). 2009.

[9] Khabbazian, Majid, Hugues Mercier, and Vijay K. Bhargava. "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks." IEEE Transactions on Wireless Communications 8.2 (2009): 736-745.

[10] Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks." Computer networks 51.13 (2007): 3750-3772.

[11] Gupta, Saurabh, Subrat Kar, and S. Dharmaraja. "WHOP: Wormhole attack detection protocol using hound packet." Innovations in information technology (IIT), 2011 international conference on. IEEE, 2011.

[12] Tun, Zaw, and Aung Htein Maw. "Wormhole attack detection in wireless sensor networks." World Academy of Science, Engineering and Technology46 (2008): 2008.

[13] Hu, Lingxuan, and David Evans. "Using Directional Antennas to Prevent Wormhole Attacks." NDSS. 2004.

[14] Lee, Gunhee, Jungtaek Seo, and Dong-kyoo Kim. "An approach to mitigate wormhole attack in wireless ad hoc networks." Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, 2008.

[15] Sadeghi, Mohammad, and Saadiah Yahya. "Analysis of Wormhole attack on MANETs using different MANET routing protocols." Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on. IEEE, 2012.

[16] Arora, Mani, Rama Krishna Challa, and Divya Bansal. "Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks." Computer

and Network Technology (ICCNT), 2010 Second International Conference on. IEEE, 2010.

[17] Jain, Shalini, and Satbir Jain. "Detection and prevention of wormhole attack in mobile adhoc networks." International Journal of Computer Theory and Engineering 2.1 (2010): 78.

[18] Chen, Honglong, Wei Lou, and Zhi Wang. "Conflicting-set-based wormhole attack resistant localization in wireless sensor networks." Ubiquitous Intelligence and Computing (2009): 296-309.

[19] Chiu, Hon Sun, and King-Shan Lui. "DelPHI: wormhole detection mechanism for ad hoc wireless networks." Wireless pervasive computing, 2006 1st international symposium on. IEEE, 2006.