Asian Journal of Information Technology 16 (1): 77-81, 2017
ISSN: 1682-3915

An Enhanced Method to Detect and Prevent Wormhole Attack in m-Commerce

S.M. Udhaya Sankar, V. Vijaya Chamundeeswari and Jeevaa Katiravan
Department of Computer Science and Engineering, Velammal Engineering College,
Chennai 66, Tamil Nadu, India

Abstract: M-Commerce applications show great potential and strategic implication of global trade and effective way of information exchange as a trade using mobile internet. The openness of wireless networks and mobility of mobile nodes and terminals have brought many advantages for the development of mobile commerce. Currently, many researchers have concentrated on the new or vital security requirements of mobile commerce. But still the safety of using mobile commerce has become bottleneck. Some recent studies bring a particular serious attack, called wormhole attack which mainly affects the wireless-based systems and may also occur in m-Commerce systems. Although, there are many solutions to confront wormhole attack in the field of wireless environment, the solution still have some problems to be overcome in m-Commerce environment. In this study we present an enhanced method called heuristic which consists of two solutions: T-Pac and T-Cut. The former can detect the presence of wormhole attack and the latter can prevent and avoid the existence of wormhole attack in m-Commerce wireless based environment. Our simulation result shows that our proposed mechanism is more effective in avoiding wormhole attack and reduces the traffic in the network.

Key words: Mobile commerce, wormhole attack, heuristic algorithm, networks, wireless

INTRODUCTION

One of the fast growing technologies in mobile communication is mobile commerce. Mobile commerce also known as m-Commerce is a kind of e-Commerce which combines Internet with the mobile communication devices such as mobile phone, PDA, smart phones etc. Users can seek, select and purchase goods and services by their mobile phones, wireless terminals or PDA (Personal Digital Assistant) anywhere or anytime without the limitation of PC or connecting line. The m-Commerce provides services such as: banking business, purchasing, marketing and advertising, trade, shopping, services based on location and entertainment (Yuan and Xinglin, 2011) and is easier, more flexible and convenient compared with traditional e-Commerce. The m-Commerce is being seen as a new wave and dimension of making business. The reasons for these developments can be traced back mainly due to faster data transmission technologies and better mobile devices prepared with enhanced computing capacity, enhanced data storage and better user-interface. There are dual security risks in wireless network during the transaction process. The problem of pay for safety becomes a barrier of the m-Commerce development. The high availability of mobile conceptual background to clarify the connection between m-Commerce and phones which is greater than that of computers in most countries is leading to concepts of new, innovative mobile services, collectively described as m-Commerce related fields. Usually mobile payment as shown in Fig. 1, the customer can communicate with the server through text message or through WAP. If the customer uses text message, the information sent goes through the SMS gateway. The SMS gateway receives, interprets and forwards the message to the server. On the other hand, if the user tries to connect to the system through WAP, the request and response goes via the WAP gateway. The gateway converts the requests from the cellular-based network devices to the format that would be understood by the IP-Based network device and vice-versa.

The mobile payment schemes are classified into three different methods. The first method is an alternative payment method on internet. Users can use their phone to complete their transactions by giving their cell phone number and they will be charged on their mobile carrier phone bill. A second method of mobile payment is to pay at a POS (Point of Sale) with a mobile phone. Consumers must bring into line with the merchant system to complete a transaction. The third method is payment for mobile commerce applications. In this method of mobile payment, the user chooses what he/she wants to buy and conducts the transaction with a secure mobile payment system. The main advantage of this method is that consumers can pay anytime, anywhere (Tabandehjooy and Nazhand, 2010).

Corresponding Author: Udhaya Sankar, Department of Computer Science and Engineering, Velammal Engineering College, Chennai 66, Tamil Nadu, India.

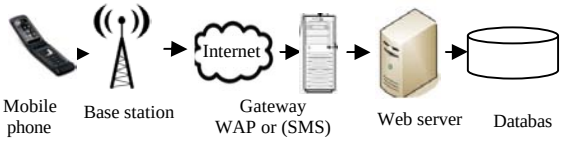

Fig. 1: A simple architecture of m-Commerce

The m-Commerce application can run in ad hoc networks in which all users and servers such as banks, customers, Certificate Authority (CA) and merchants can communicate through mobile devices which are portable thus gaining increasing acceptance. A customer makes transaction with a merchant using his/her mobile device while the bank plays the key role in handling the transaction between the customer and the merchant. The customer can connect to the Point of Sale (POS) or to the base station through his/her mobile phone as shown in Fig. 2. The merchant will receive the transaction message directly from the customer's mobile phone or indirectly through peer mobile devices (Pai and Wu, 2009).

The open nature of the mobile medium and since the message passes through peer mobile devices, it makes easy for outsiders to overhear to network traffic which makes the attacker to easily interfere into the network. These factors make mobile networks potentially vulnerable to several different types of malicious attacks such as wormhole attack. In this study, we define the wormhole attack that exists in mobile commerce environment through mobile nodes and we present effective mechanisms to detect and prevent the presence of wormhole attack in the network.

Wormhole attack in mobile commerce: A wormhole attack is particularly severe attack on ad hoc networks and now it has been encountered in m-Commerce environment which is aimed at damaging the routing function of wireless and ad hoc networks. A wormhole attack occurs when there exists two or more colluding attackers and wormhole tunnel in the network which are connected by the high speed off-channel links. Once the wormhole tunnel is established, the adversary records the packets it overhears and forwards the packet to the other end of the network through the wormhole tunnel. The existence of tunnels is beneficial because it increases the total capacity of the network and adversaries may fabricate false routes to deceive other nodes, breaking the coordination of routing protocol and disabling the communication abilities of nodes, severely damaging the network. Furthermore, the wormhole nodes can snoop on the network and use the information they gather to masquerade as legitimate nodes (Pai and Wu, 2011). We divide the wormhole attack into two different categories: hidden wormhole attack and exposed wormhole attack (Su and Boppana, 2008). The hidden wormhole attack is

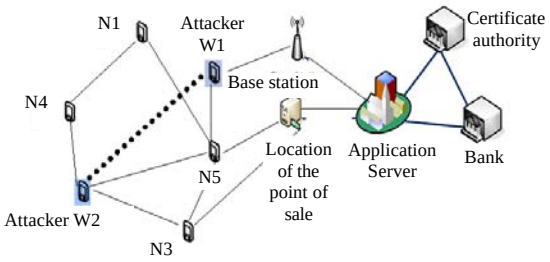

Fig. 2: Wormhole attack in mobile commerce

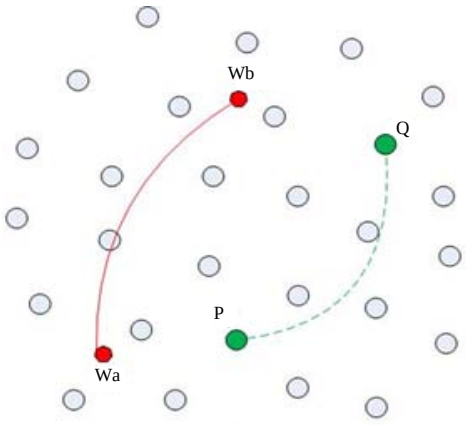

Fig. 3: Wa and Wb is a hidden wormhole attack that is connected through a wired link; PQ is an exposed wormhole attack

the traditional wormhole attack in which the colluding nodes records the packets and retransmits them. This attack can be easily mounted by introducing the hardware without compromising any host in the network. Exposed wormhole attack is called byzantine wormhole attack in which the attacker injects two colluding nodes at the ends in the network and a wormhole link is built by the attacker between the two colluding nodes. The link so created forms a wormhole. The tunneling procedure generates an illusion that the two nodes more than one hop away are in the neighborhood of each other. This illusion determines shortest choke points that are under the control of the attacker and can be utilized in future to degrade, disrupt or analyze the traffic stream (Fig. 3).

We use an example given in Fig.4 to show the working of wormhole attack in the network. Fig. 4 is the network that comprises a pair of colluding nodes W1 and W2 which has the tunnel between them and other nodes namely, N1-N6. Suppose that S broadcasts a route request message to find the secure path for communicating with node D and if the attacker W1 receives the message it forwards the received message along with additional

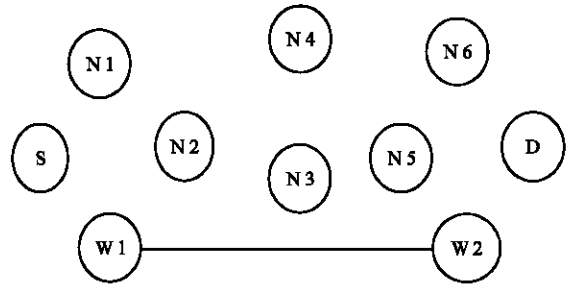

Fig. 4: Working of wormhole attack

eavesdropped information through the wormhole tunnel to the other attacker W2. The false message will reach the destination D before the arrival of the original route request through other paths. When the destination D receives this false messages it returns a route reply message to the source S through the same wormhole tunnel. At this moment, the attacker W2 also receives this reply message and forwards the message with its eavesdropped information to attacker W1 which again transmits it to the source S.

Literature review: Sharma and Trivedi (2011) proposed the use of digital signature for detecting wormhole node. When the sender broadcasts the request it adds the digital signature along with the request. The node which receives the request compares the digital signature of the sending node from its database. If the signature is matched, the sender is the legitimate node and the receiving node also adds its signature and forwards to the next node. If the signature is not matched then the node that receives the request discards it and informs to all the nodes in the network and updates in the database, because malicious node contains either duplicate signature or no signature.

SECTOR proposed by Wang and Wong (2007) that used Mutual Authentication with Distance-Bounding (MAD) protocol to find their true neighbors by determining their mutual distances when they meet one another. MAD uses two bit nodes: one node first sent out one bit which is considered as a challenge and then another node responds with one bit immediately after receiving the challenge. By measuring the time between sending out a challenge and receiving the response, the first node can compute an upper bound of the distance between these two nodes and then check if this distance violates any physical constraints.

Chen *et al.* (2010) in his study had proposed a Secure Localization scheme Against Wormhole attack (SLAW). This scheme includes three phases: wormhole attack detection, neighboring locators differentiation and secure localization. The main idea behind the secure localization is to build conflicting-sets for each locator according to the abnormalities of message exchanges among neighbor locators which is used to differentiate the uncertain locators from valid locators. The procedure of the SLAW is shown as follows:

- When the sensor receives messages from neighboring locators, it runs wormhole attack detection process
- If the wormhole attack is detected then the sensor runs neighboring locators differentiation process
- The sensor runs secure localization process. Thus in this work, the severe impacts of the wormhole attack on the localization in hostile wireless sensor networks was analyzed

Hu *et al.* (2006) in his researcher presented a general mechanism called packet leashes for detecting and defending against wormhole attack. It presents a protocol called TIK that implement leashes. Leashes are designed to protect against wormholes over a single wireless transmission; when the packets are sent over multiple hops, each transmission requires the use of a new leash. This technique allows the receiver of a packet to detect if the packet travelled further than the leash allows.

Abdesselam *et al.* (2008) attempts to pinpoint links that may potentially be a part of wormhole tunnel. The links that experience long delays are treated as suspicious links. As such, wormhole verification must be performed only on such suspicious links. After detecting suspicious links, the originator estimated hop count; the sender predicts the wormhole attack. Then, the wormhole tracking starts after the wormhole is detected in the network. It performs a verification procedure for each suspicious link to check whether there is any wormhole tunnel sitting along the path between itself and the other end point of the suspicious link. To detect the wormhole tunnel, the node sends probing packets to all of its suspect nodes. When a node receives the probing packet, it replies with an ACK message to the originator of the probing packet after stopping all transmission of data packets.

Su and Boppana (2010) presented NEVO (Neighbor Verification by Overhearing) in which nodes passively monitor (overhear) the forwarding of broadcast type packets by their neighbors and use the send and overhear times of transmission of these packets to mitigate these wormhole attacks. NEVO can detect almost all instances of wormhole attacks and is virtually independent of the routing protocol used. The timing analysis of wormhole attacks is first calculated by using an algorithm. Then the NEVO protocol that facilitates message transmission sequence was presented.

Azer (2011) had proposed scheme that relies on the idea that usually the wormhole nodes participate in the routing in repeated way as they attract most of the traffic.

Therefore, each node will be assigned cost depending in its participation in routing. A node that has been used more than once has its cost increased linearly. This is to ensure that a tempting path that offers apparently small number of hops will have a high cost because it contains a node that was used before. This solution has the privilege of providing a load balance in the ad hoc networks which saves regular nodes from resource consumption, if they repeatedly participate in the routing.

Wang and Wong (2007) proposed a mechanism which is based on the smallest hop count estimation between source and destination. If the hop count of a received shortest route is much smaller than the estimated value an alert of wormhole attack is raised at the source node. The sender sends the RREQ to the receiver by setting the flag. Once the receiver receives the RREQ, it responds to the sender by sending RREP and its current position. The sender retrieves the receiver's current position and it estimates the shortest path in terms of hop count. If the received hops count value is lesser than the estimated hop count, the sender predicts the wormhole attack. Then the wormhole tracking starts after the wormhole is detected in the network.

Hu and Evans developed a protocol using directional antennas to prevent wormhole attacks. Directional antennas are able to detect the angle of arrival of a signal. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e., one from West and the other at East). This protocol fails only if the attacker strategically placed wormholes residing between two directional antennas.

MATERIALS AND METHODS

Proposed work

Heuristic algorithm: The constructive heuristic algorithm is proposed for detecting wormhole attack. Heuristic refers to experience-based techniques for problem solving, learning and discovery. The objective of this algorithm is to find the optimal of all possible solutions that is one that minimizes or maximizes an objective function. Heuristic methods are used to speed up the process of finding a satisfactory solution. These algorithms can be accurate that is they actually find the best solution. It significantly reduces overhead and enables further and more detailed analysis on potentially malicious code. Heuristic algorithm is capable of detecting a wide variety of attacks. In this research heuristic algorithm uses two concepts for detecting wormhole attack. They include: T-Pac, T-Cut.

T-Pac: The T-Pac is abbreviated as tour packing heuristics. The tour packing heuristic algorithm is the one that constructs a solution by iteratively adding one node to the solution at a time, in an order determined by a pre-defined cost. The time taken for adding a node is estimated initially. More precisely, the algorithm starts from the sink node and in each iteration, attempts to add a node to an existing network as long as the time constraints remain satisfied. The nodes in the network are added and the time taken for adding the nodes is calculated. The time initially estimated and the time taken for adding each node is compared and the malicious node is identified if any discrepancy occurs. The T-Pac algorithm is extended for detecting wormhole attack by monitoring the path through which the packets are sent. It identifies the intruders and gives the details about their mobility in the network.

T-Cut: The T-Cut is abbreviated as tour cutting heuristics algorithm. This algorithm cuts the network into individual nodes to detect and block the wormhole node or link and prevents the network from attacks. The time taken to cut all the nodes is calculated. In T-Cut algorithm we cut each node in the network and check whether the time for cutting each node is equivalent to the time calculated initially. If there is a discrepancy then we predict the presence of wormhole attack in the network.

RESULTS AND DISCUSSION

The proposed scheme has prevented the routing through the wormhole nodes on the expense of the increase of end to end delay. From the simulation results, the attack was prevented as before by forbidding the malicious node to dominate the routing operation continuously. Moreover as we can see from Fig. 5 and 6 that using heuristics helps save the time thereby preventing the end-end delay in the network that it is

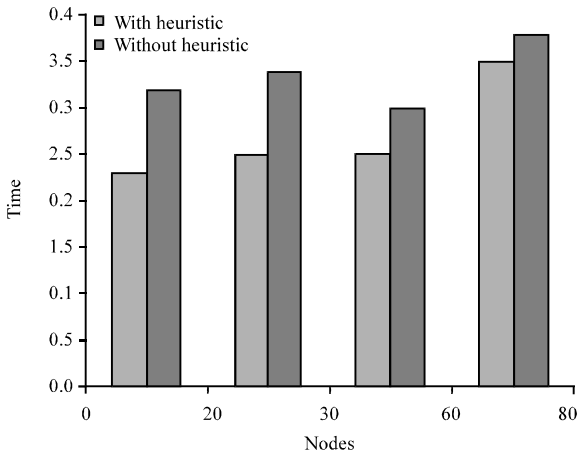

Fig. 5: Comparing time versus nodes with and without heuristics

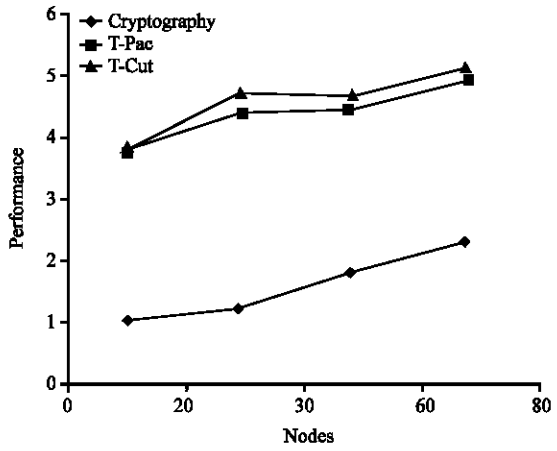

Fig. 6: Performance of our proposed technique with the existing cryptography theories

deployed. Comparing the end to end delay with cryptography parameters proves a significant increase in performance of the network. Cryptographic keys and parameters will significantly impose an additional 21% time delay. Since, our proposed method doesn't use keys and parameters to detect wormhole attack, a significant performance improvement in the network can be observed.

CONCLUSION

The wormhole attack is prominent attack that affects the entire network. In order to avoid such vulnerable attack we present heuristic algorithm which uses T-Pac for identifying and monitoring the malicious node and T-Cut for detecting and cutting the wormhole attack from the network. Heuristic algorithm works with all known ad hoc routing protocols and takes the advantage of the reducing traffic in the network which causes the pathway for the wormhole attack entering in the network. Our simulation results shows that T-Pac and T-Cut is highly effective against wormhole attack and no routes used for data packets go through wormholes. To sum up, our proposed technique proactively addresses and overcomes the security challenges in the field of mobile commerce.

REFERENCES

Abdesselam, F.N., B. Bensaou and T. Taleb, 2008. Detecting and avoiding wormhole attacks in wireless ad hoc networks. IEEE. Commun. Mag., 46: 127-133.

Azer, M.A., 2011. Wormhole attacks mitigation in ad hoc networks. Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES), August 22-26, 2011, IEEE, Cairo, Egypt, ISBN: 978-1-4577-0979-1, pp: 561-568.

Chen, H., W. Lou and Z. Wang, 2010. Secure localization against wormhole attacks using conflicting sets. Proceedings of the IEEE 29th International Performance Computing and Communications Conference, December 9-11, 2010, Albuquerque, NM., USA., pp: 25-33.

Hu, Y.C., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE. J. Sel. Areas Commun., 24: 370-380.

Pai, H.T. and F. Wu, 2009. Preventing wormhole attacks in mobile commerce. Proceedings of the IEEE International Conference on E-Business Engineering (ICEBE'09), October 21-23, 2009, IEEE, Chiayi, Taiwan, ISBN:978-0-7695-3842-6, pp: 437-442.

Pai, H.T. and F. Wu, 2011. Prevention of wormhole attacks in mobile commerce based on non-infrastructure wireless networks. Electronic Commerce Res. Appl., 10: 384-397.

Sharma, P. and A. Trivedi, 2011. An approach to defend against wormhole attack in ad hoc network using digital signature. Proceedings of the IEEE 3rd International Conference On Communication Software and Networks (ICCSN), May 27-29, 2011, IEEE, New York, USA., ISBN:978-1-61284-485-5, pp: 307-311.

Su, X. and R.V. Boppana, 2008. Mitigating wormhole attacks using passive monitoring in mobile ad hoc networks. Proceedings of the IEEE Conference on Global Telecommunications GLOBECOM, November 30- December 4, 2008, IEEE, San Antonio, Texas, ISBN:978-1-4244-2324-8, pp: 1-5.

Tabandehjooy, A.A. and N. Nazhand, 2010. A lighweight and secure protocol for mobile payments via wireless internet in m-commerce. Proceedings of the International Conference on E-Education, E-Business, E-Management and E-Learning (IC4E'10), January 22-24, 2010, IEEE, Shiraz, Iran, ISBN: 978-1-4244-5680-2, pp: 495-498.

Wang, X. and J. Wong, 2007. An end-to-end detection of wormhole attack in wireless ad-hoc networks. Proceedings of the 31st Annual International Conference on Computer Software and Applications Conference (COMPSAC07), Vol. 1, July 24-27, 2007, IEEE, New York, USA., ISBN: 0-7695-2870-8, pp: 39-48.

Yuan, M. and D. Xinglin, 2011. The realization of pay for safety of M-commerce based on WAP. Proceedings of the 2011 International Conference on E-Business and E-Government (ICEE), May 6-8, 2011, IEEE, Qingdao, China, ISBN: 978-1-4244-8691-5, pp: 1-3.