International Journal of Soft Computing 13 (1): 1-5, 2018
ISSN: 1816-9503

Secured Transmission for PMIPv6 Based Network Mobility using PlGPA Protocol

[1]S. Kayaivizhi and [2]M. Ponnavaikko
[1]Easwari Engineering College, Chennai, India
[2]Bharath University, Chennai, India

Abstract: PMIPv6 is a network based mobility management protocol responsible for managing IP mobility on behalf of the host. In this study, a protocol called PLGPA is implemented to reduce the consumption of the battery power in PMIPv6 . PLGPA adds a verifiable path history to every PLGP packets. PLGPA uses this packet history together with PLGP's tree routing structure so that every node can securely verify progress. A secured ECC based authentication scheme integrated with PLGPA is also proposed. This research proxy mobile IPv6 domain refers to the network where the mobility management of a mobile node is handled using the proxy mobile IPv6 protocol. It is responsible for managing IP mobility on behalf of the host. Major security threats found in PMIPv6 are man-in-the-middle attack, traffic redirection attack, resource depletion attack etc., This study concentrates on the resource depletion attack called vampire attack which causes draining of battery by a suspicious node on activated nodes in PMIPv6. This research is being carried out using the network simulation tool OMNeT++ 4.0.

Key words: Proxy Mobile IPv6 (PMIPv6), Parno Luk Gaustad and Perrig with attestation (PLGPA), Denial of Service (DOS), Elliptical Curve Cryptography (ECC), Vampire, depletion

INTRODUCTION

Vampire attacks make a network to consume more time and energy to transmit the data, compared to transmission by honest nodes and a node is permanently disabled once its battery power is exhausted. Vasserman and Hopper (2013) described about Vampire attacks which drains life from wireless ad hoc sensor networks. Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. Resource depletion attacks at the routing protocol layer permanently disable networks by quickly draining nodes battery power (Deshmukh and Potgantwar, 2015). These Vampire attacks are not specific to any specific protocol but rather rely on the properties of many popular classes of routing protocols. There are two types of Vampire attack:

- Carousel attack where adversary sends packets with routes composed of a series of loops
- Stretch attack where adversary constructs artificially long routes traversing every node in the network

In Carousel attack, adversary sends packets with routes composed of a series of loops as shown in Fig. 1.

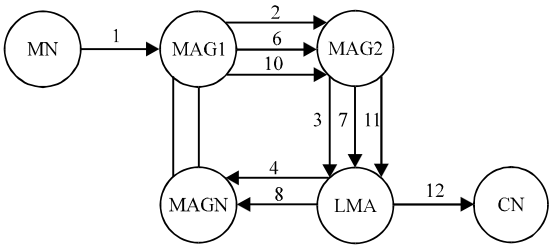

Fig. 1: Carousel attack

It exploits limited verification of message headers at forwarding nodes. It is used to increase the route length beyond no. of nodes in network.

In stretch attack, adversary constructs artificially long routes traversing every node in the network as shown in Fig. 2. It causes packets to traverse larger than optimal no. of nodes. It makes the nodes that don't lie on optimal path to process packets. It is potentially less damaging per packet than the carousel attack.

Proxy Mobile IPv6 (PMIPv6) is the protocol which provides mobility of mobile node in the network without the participation of mobile node in IP related signaling. All the mobility signaling and setting up the required routing state is done by mobility entities in the network. There are numerous security attacks in PMIPv6 like resource

Corresponding Author: S. Kayaivizhi, Easwari Engineering College, Chennai, India

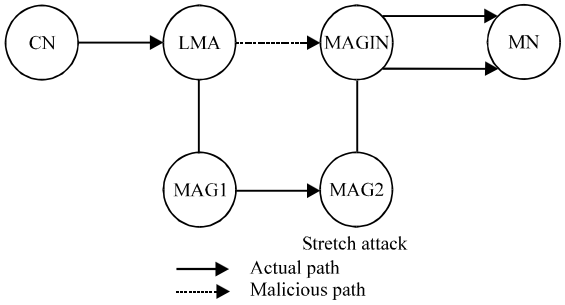

Fig. 2: Stretch attack

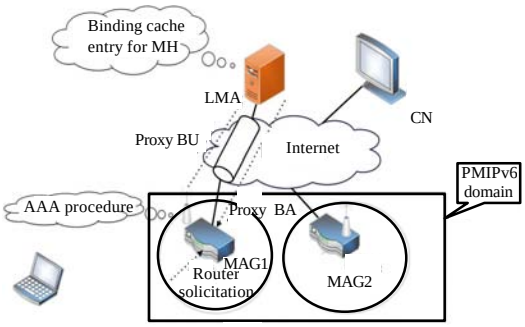

Fig. 3: PMIPv6 operation

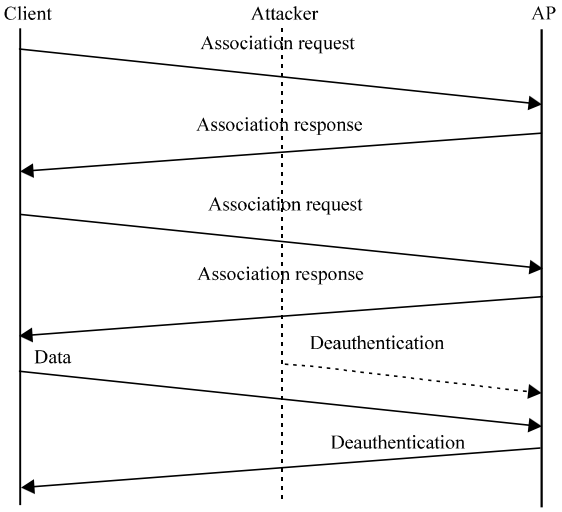

Fig. 4: DOS attack between client and AP

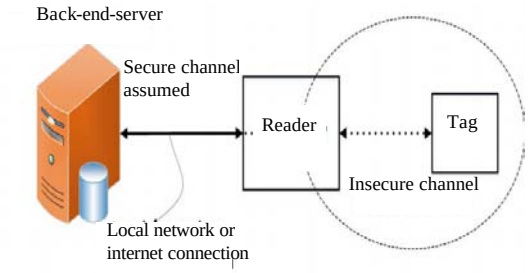

Fig. 5: RFID system

depletion attacks, DOS attacks, etc. To overcome the security issues PLGP and PLGPA protocol is implemented and ECC based algorithm is used to further enhance the security.

Sinan *et al*. (2008) presented an overview of the handover process in MIPv6. Here, each node in MIPv6 has a home network and an IPv6 home address assigned to MN within the network prefix of the home network. The MN's IPv6 home address does not change regardless of where MN is. The MN acquires a Care of Address (CoA) when it moves away from the home network. The MIPv6 protocol requires registration of CoA with the home agent thereby giving the home agent the current point of attachment to the mobile node. The correspondent node maintains a mapping of the home address and the care of address of the mobile node. The mobile node updates the mapping to the correspondent node by sending binding update messages whenever it receives packets from the home agent as shown in Fig. 3. But MIPv6 suffers from significant overhead in increased delay, packet loss and signaling cost when the MN changes the point of attachment to the network frequently (Lee *et al*., 2012; Ryu *et al*., 2004).

Bellardo and Savage (2003) proposed real vulnerabilities of denial-of-service attacks and its practical solutions as shown in Fig. 4. The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors.

However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11s basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. It has been suggested that 802.11 is highly susceptible to malicious Denial-of-Service (DoS) attacks targeting its management and media access protocols.

Peris-Lopez *et al*. (2006) proposed a minimalist mutual-authentication protocol for low-cost RFID tags low-cost Radio Frequency Identification (RFID) tags affixed to consumer items as smart labels are emerging as history. This presents a number of advantages but also one of the most pervasive computing technologies in opens a huge number of security problems that need to be addressed before its successful deployment. RFID system is shown in Fig. 5. Many proposals have recently appeared but all of them are based on RFID tags using classical cryptographic primitives such as Pseudorandom Number Generators (PRNGs), hash functions or block ciphers. This assumption is fairly unrealistic as classical cryptographic constructions lie well beyond the computational reach of very low-cost RFID tags.

MATERIALS AND METHODS

Proxy mobile IPv6 domain refers to the network where the mobility management of a mobile node is handled using the Proxy mobile IPv6 protocol. It is responsible for managing IP mobility on behalf of the host. Major security threats found in PMIPv6 are man in the middle attack, traffic redirection attack, resource depletion attack etc., The proposed research concentrates on the resource depletion attack called vampire attack which causes draining of battery by a suspicious node on actuated nodes in PMIPv6. A protocol called PLGPA is implemented to reduce the consumption of the battery power in PMIPv6 (Fig. 6). PLGPa adds a verifiable path history to every PLGP packets. PLGPA uses this packet history together with PLGP's tree routing structure so that every node can securely verify the progress.

Elliptic Curve Cryptosystem (ECC) based algorithms would be best choice algorithms due to their small key sizes and efficient computations. A secured ECC based authentication scheme integrated with PLGPA is also proposed. This work is being carried out using the network simulation tool OMNeT++ 4.0.

The core functional entity in PMIPv6 are Local Mobility Anchor (LMA) and Mobility Access Gateway (MAG). The LMA's responsibility is to maintain mobile mode's reachability state. The responsibility of MAG is to detect the mobile node's movement into access network and out from access link and it initiates the binding registrations to the mobile node's LMA. Vampire attack makes a network to consume more time and energy to transmit the data, compared to the transmission by honest nodes. This work deals with attack-resistant minimal energy routing where the adversary's goal includes decreasing energy savings. PLGPA protocol is given as:

- MN transfers data packet to the MAG
- MAG consists of PLGP protocol with attestation that transfers data to LMA. LMA verifies whether the data matches the source node. If not, it is sent to MAG
- LMA verifies whether the data matches the source node. If it matches, it transmits the data to CN
- LMA adds a verifiable path history to every PLGP packet. PLGPA uses this packet history together with PLGP's tree routing structure

Every node securely verifies the progress, preventing any significant adversarial influence on the path taken by any packet which traverses atleast one honest node. These signatures form a chain attached to every packet, allowing any node receiving, it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination. ECC based security is used for encryption and decryption of PLGP to provide security.

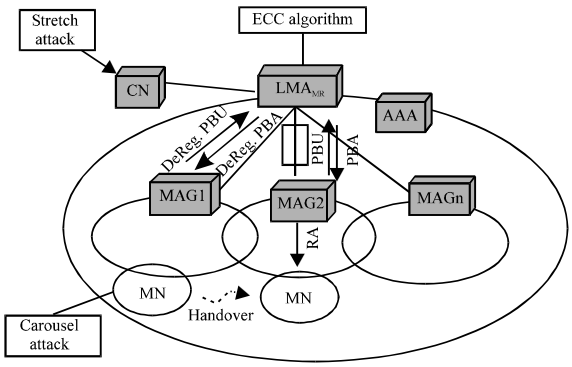

Fig. 6: Proposed system

RESULTS AND DISCUSSION

Network setup is created to simulate the carousel and stretch attacks. Energy usage with various attacks are studied. Performance metrics like end-to-end delay and delivery ratio are observed.

Carousel attack simulation: Carousel attack simulation is shown in Fig. 7. Initially the source node starts transmission. The source node sends packets to the sink node.

Stretch attack simulation: Stretch attack simulation is shown in Fig. 8. The source node sends packet to the sink after creating an artificially long route. It traverses the packets in the long route for a long time and finally sends the packet to the sink.

Energy usage with various attacks: Table 1 gives the node energy distribution under various attack scenarios. The network is composed of 30 nodes and a single randomly positioned vampire. Results shown are based on a single packet sent by the attacker. The results show that energy consumption by carousel attack is more. Current research in minimal energy routing which aims to increase the life time of power constrained networks by using less energy to transmit and receive packets. However, Vampires will increase energy usage even in minimal energy routing scenarios and when power conserving MAC protocols are used. These attacks cannot be prevented at the MAC layer or through cross layer feedback. Attackers will produce packets which traverse more hops than necessary, so, even if nodes spend the minimum required energy to transmit packets, each packet is still more expensive to transmit in the presence of Vampires. The above parameter is considered in the analysis of this research.

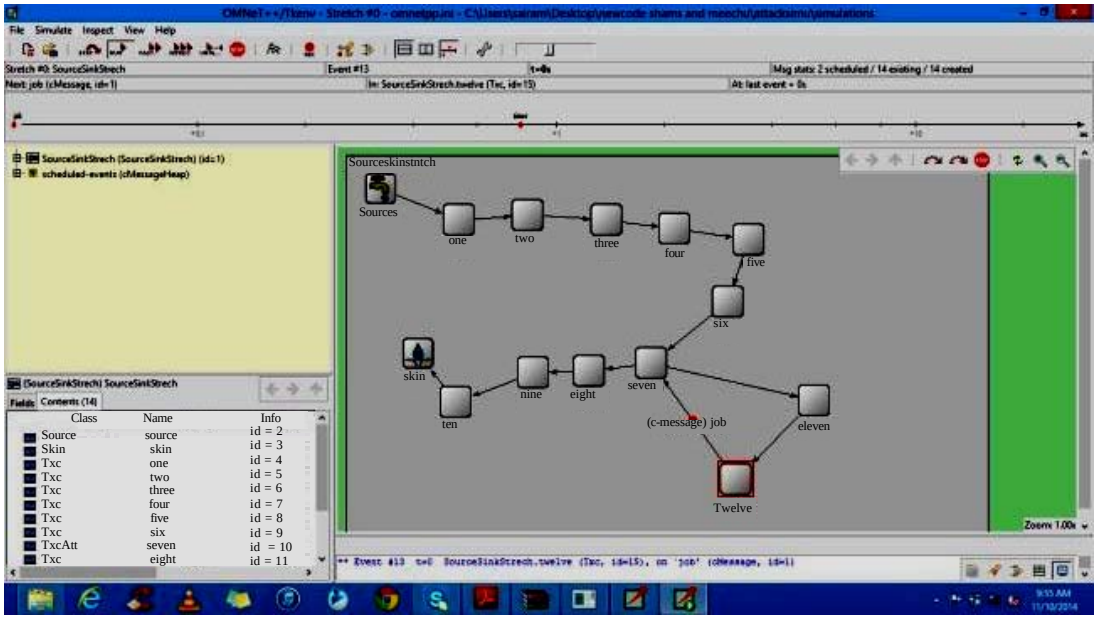

Fig. 7: Carousel attack simulation

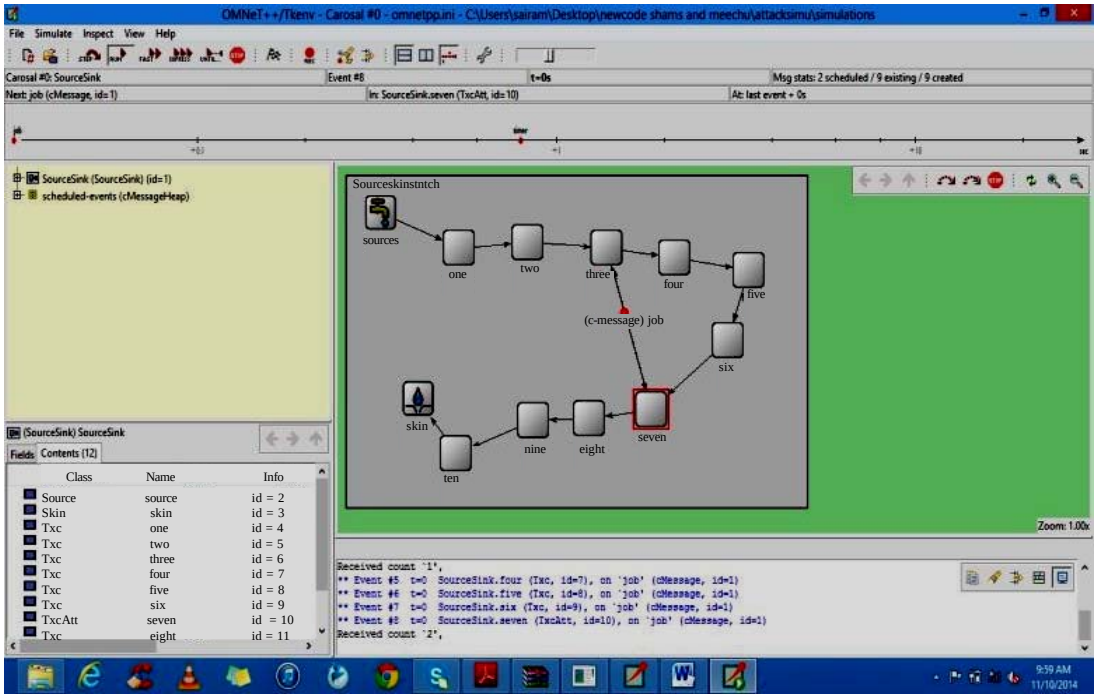

Fig. 8: Stretch attack simulation

Table 1: Node energy distribution under various attacks

Nodes	Fraction of total nodes	Fraction of node energy consumed
Honest node	0.90	0.01
Stretch attack node	0.80	0.02
Carousel attack node	0.60	0.07

Energy usage with stretch attacker: Every network node, causing an energy usage increase of factor 0 (min (N, λ)) where N is the number of nodes and λ is the maximum path length allowed. This attack is potentially less damaging per packet than the carousel attack as the

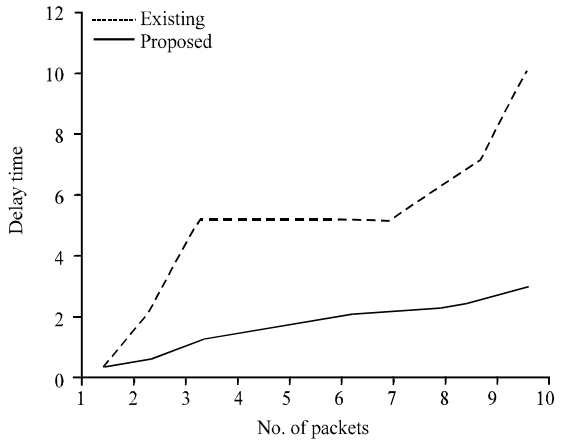

Fig. 9: End to end delay

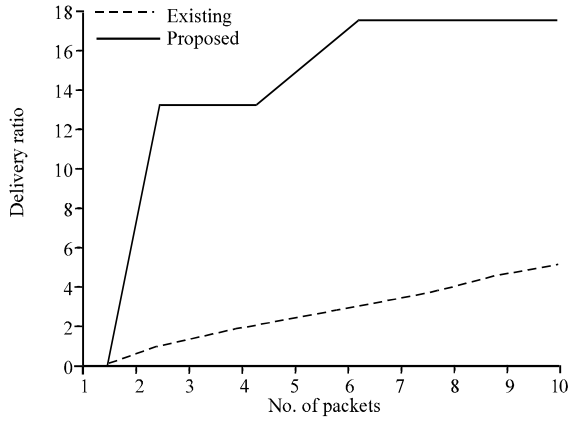

Fig. 10: Delivery ratio

number of hops per packet is bounded by the number of network nodes. Table 2 shows the effects of a single node stretch attacker on a network of 30 nodes. Maliciousness is measured in terms of the induced stretch of the optimal route in number of hops.

Performance metrics

End to end delay: End to end delay is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by the battery depletion by the impact of vampire attack. Figure 9 shows that the end-to-end delay is comparatively low in the proposed system:

$$\text{End to end delay} = \frac{\sum \text{Number of packets received}}{\sum \text{Number of packets sent}}$$

Delivery ratio: Delivery ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets sent. Figure 10 shows that the delivery ratio is improved in the proposed system.

Table 2: Effects of single node stretch attack

Packets	Fraction of energy consumed	Malicious route stretch (hops)
1	Low	Low
10	Low	Low
100	Fair	Fair
1000	High	High
10000	High	High

CONCLUSION

Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable wireless networks by depleting node's battery power. A new scheme PLGPA is proposed in this study to add a verifiable path history to every PLGP packet. PLGPA uses this packet history together with PLGP's tree routing structure, so that, every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Simulations on carousel attack and stretch attack were carried out and the results show that the performance of PLGPA protocol in PMIPv6 network is better than the existing one.

REFERENCES

Bellardo, J. and S. Savage, 2003. 802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions. Proceedings of the 2003 USENIX Symposium on Security Vol. 12, August 4-8, 2003, USENIX Association, Berkeley, California, pp: 1-2.

Deshmukh, L.R. and A.D. Potgantwar, 2015. Ensuring an early recognition and avoidance of the vampire attacks in WSN using routing loops. Proceedings of the 2015 IEEE International Conference on Advance Computing Conference (IACC'15), June 12-13, 2015, IEEE, Banglore, India, ISBN:978-1-4799-8048-2, pp: 61-66.

Lee, J.H., T. Ernst and N. Chilamkurti, 2012. Performance analysis of pmipv6-based network mobility for intelligent transportation systems. IEEE Trans. Veh. Technol., 61: 74-85.

Peris-Lopez, P., J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, 2006. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. Ubiquitous Intell. Comput. Lecture Notes in Comput. Sci., 4159: 912-923.

Ryu, S., K.J. Park and J.W. Choi, 2004. Enhanced fast handover for network mobility in intelligent transportation systems. IEEE. Trans. Veh. Technol., 63: 357-371.

Sinan, S., M. Ismail and K. Jumari, 2008. A comparison of mobile node's handoff between mobile IPv6 and fast handover protocol. J. Inst. Eng. Malaysia, 69: 27-30.

Vasserman, E.Y. and N. Hopper, 2013. Vampire attacks: Draining life from wireless ad hoc sensor networks. IEEE. Trans. Mob. Comput., 12: 318-332.