International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

Detecting Identity Based Attack in MIMO System Using Link Signature in Wireless Network

Kanimozhi.V[1], keerthana.D[2],Sri Devi.G[3],Panimalar.S[4]

[1,2,3]Dept. of Computer Science & Engineering, Panimalar Institute Of Technology, Chennai,Tamilnadu, India
[4]S.Panimalar ,Assistant Professor, Dept. of Computer Science & Engineering, Panimalar Institute Of Technology, Chennai,Tamilnadu, India

----------***----------

Abstract-*Wireless link signature is becoming increasingly important as wireless devices between a transmitter and a receiver to provide authentication of wireless signals. This project identifies a new attack, called mimicry attack, against the existing wireless link signature schemes. It is assumed in that an attacker "cannot 'spoof' an arbitrary link signature" and that the attacker "will not have the same link signature at the receiver unless it is at exactly the same location as the legitimate transmitter". The mimicry attack is extended to multiple-input multiple-output(MIMO) systems. To defend against the mimicry attack, this project has the construction for wireless link signature, called time-synched link signature, by integrating cryptographic protection and time factor into wireless physical layer features. This link signature is effective in physical layer authentication.*

KeyWords: 1.MimoSystem,2.Link Signature,3.Time-Synched

1.INTRODUCTION

Wireless physical layer security is becoming increasingly important as wireless devices are more and more pervasive and adopted in critical applications. There have been multiple proposals in recent years to provide enhanced wireless security using physical layer characteristics, including fingerprinting wireless devices, authenticating and identifying wireless channels , and deriving secret keys from wireless channel features only observable to the communicating parties . Among the recent advances in wireless physical layer security is link signature. Link signature uses the unique wireless channel characteristics between a transmitter and a receiver to provide authentication of the wireless channel.Thereare three link signature schemes . The link signature has been recognized as a physical layer authentication mechanism for applications where wireless channel characteristics is unique for individual nodes .

2.LITERATURE SURVEY:

Location distinction is the ability to determine when a device has changed its position. We explore the opportunity to use sophisticated PHY-layer measurements in wireless net- working systems for location distinction. We first compare two existing location distinction methods one based on channel gains of multi-tonal probes, and another on channel impulse response. Next, we combine the benefits of these two methods to develop a new link measurement that we call the complex temporal signature. We use a 2.4 GHz link measurement data set, obtained from CRAWDAD , to evaluate the three location distinction methods. We find that the complex temporal signature method performs significantly better compared to the existing methods. We also perform new measurements to understand and model the temporal behavior of link signatures over time. We intergrate our model in our location distinction mechanism and significantly reduce the probability of false alarms due to temporal variations of link signatures.

3.EXISTING SYSTEM:

Existing techniques using non-cryptographic approaches to authenticate wireless transmitters can be classified into three categories: software

fingerprinting, location distinction, and radiometric identification. The RSS based methods directly estimate the location of a signal origin using the RSS values. However, such methods can be defeated with an array antenna, which can fake arbitrary source locations. The link signature based approaches authenticate the channel characteristics between the transmitter and the receiver. In radiometric identification approaches, the distinctive physical layer characteristics exhibited by wireless devices are utilized to distinguish between them .

3.1DISADVANTAGES:

- Existing wireless link signature schemes not suitable for mimicry Attacks.
- Attacker utilizing at least the same number of antennas as the receiver's antennas can successfully launch the mimicry attack. Cannot easy to identifying mimicry attacks.
- It has Less Security from mimicry attacks

4.PROPOSED SYSTEM

If the number of the receiver's receive antennas is larger than that of the attacker's transmit antennas, the receiver can detect the mimicry attack.There is the construction for link signature, which is called time synched link signature. Time-synched link signature integrates cryptographic protection as well as time factor into the wireless physical layer features, and provides an effective and practical solution for authenticating physical layer wireless signals.This project shows the threats of the mimicry attack and demonstrate the effectiveness of the time-synched link signature for physical layer authentication.

4.1ADVANTAGES:

- It is highly secure from mimicry attacks.
- Easy to identifying mimicry attacks and gives more protection from it.
- We can perform an extensive set of experiments to demonstrate both the feasibility of mimicry attacks and the effectiveness of time-synched link signature.

5.BLOCK DIAGRAM:

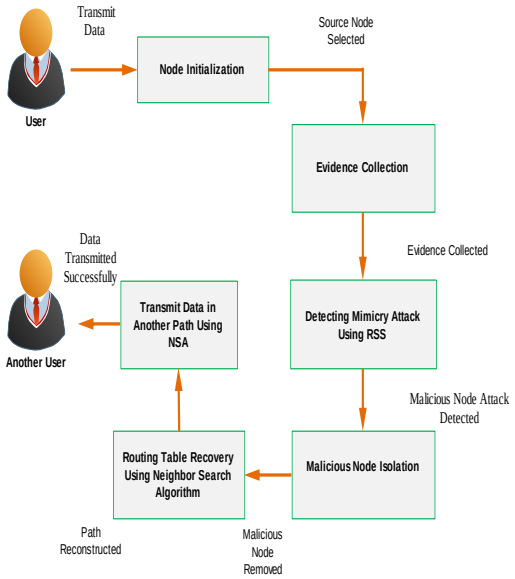


Fig -1: Block diagram of our proposed method

6.1NODE INITIALIZATION:

In this scheme, the users from various positions requesting files from the nodes in Delay Tolerant Networks.The user may access from their compromised nodes. Those compromised Nodes are captured by the adversary to leverage and for safety measures. Adversary can physically capture and compromise nodes and then mount a variety of attacks with these compromised nodes.The key idea of our scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised.

6.2 EVIDENCE COLLECTION

In this Module, We can collect the evidence of attacker node. Mimicry Attack Alert.n this module, Intrusion Time stamping gives an attack alert with a confidence value, and then RSS runs to figure out how many changes on routing table are caused by the attack.

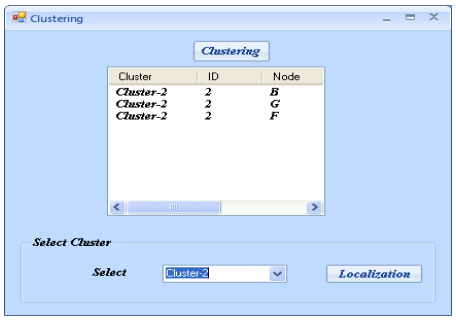
6.3 DETECTING MIMICRY ATTACK

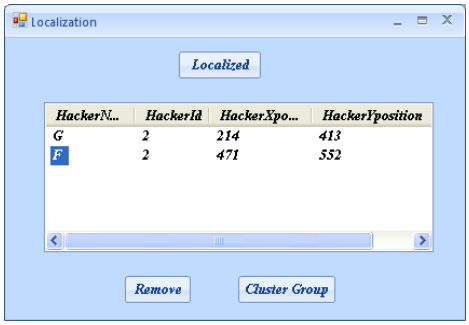
Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in Delay Tolerant Network.

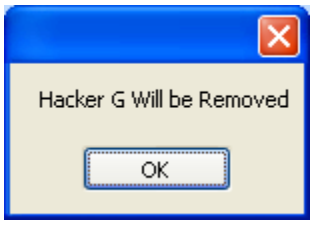
6.4 MALICIOUS NODE ISOLATION

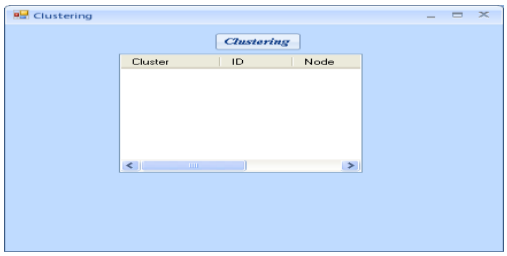
Node Isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in Delay Tolerant Network.To perform a node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting packets from it. On the other hand, a binary node isolation response may result in negative impacts to the routing operations, even bringing more routingdamages than the attack itself.

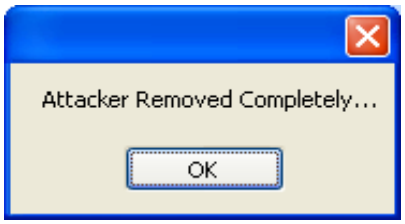
7.RESULT AND DISCUSSION:

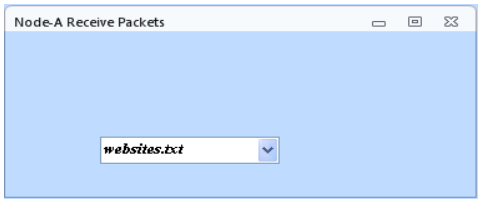


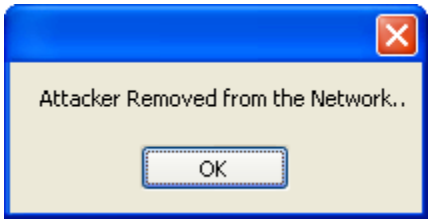












8.CONCLUSION:

In this project, we identified the mimicry attack against the existing wireless link signature schemes.We then extended the mimicry attack in MIMO systems and concluded that the attacker utilizing at least the same number of antennas as the receiver's antennas can successfully launch the mimicry attack. To defend against the mimicry attack, we proposed the novel time-synched

link signature construction by integrating cryptographic protection and time factor into wireless physical layer features. We also performed an extensive set of experiments to demonstrate both the feasibility of mimicry attacks and the effectiveness of time-synched link signature.

9.REFERENCES:

[1] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proc. ACM Workshop Wireless Secur. (WiSec), 2006, pp. 43–52.

[2] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identifi- cation with radiometric signatures," in Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 116–127.

[3] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identi- fication via analog signal fingerprinting: A matched filter approach," in Proc. 13th Annu. Symp. Netw. Distributted Syst. Secur. (NDSS), 2006, pp. 1–11.

[4] L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, "Identifying unique devices through wireless fingerprinting," in Proc. 1st ACM Conf. Wireless Netw. Secur. (WiSec), 2008, pp. 46–55.

[5] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in Proc. 13th Annu. ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2007, pp. 111–122 .