IDENTITY BASED ATTACK DETECTION AND MANIFOLD ADVERSARIES LOCALIZATION IN WIRELESS NETWORKS

UDHAYA SANKAR S.M [1], V.VIJAYA CHAMUNDEESWARI[2], JEEVAA KATIRAVAN[3]

Assistant Professor[1], Professor and Head[2], ASP[3]
Department of Computer Science and Engineering, Velammal Engineering College, Chennai.

E-mail: Udhaya3@gmail.com

ABSTRACT

Wireless spoofing attacks are easy to launch in wireless network due to openness of wireless network. Although the identity of a node can be detected through cryptographic authentication, conservative security approaches are not always possible because of their overhead requirements. Source sends a Data to the destination, Data is forwarded to the intermediate nodes in between source and destination, with respect to Received Signal Strength(RSS). In this paper to detect the identity based attacks and multiple adversaries as well as localizing the adversaries. Detect the position of multiple adversaries even when the adversaries vary their transmission power level. We propose to use the spatial correlation of received signal strength(RSS) inherited from wireless nodes to detect the attacks. We are also using primary key and encrypting the data packets during transmission for security purpose. By encrypting the data packets the intermediate nodes are not able to view the data presented in the data packets. Experiments using an 802.11 (Wi-Fi) network, We use network simulation to analyse the performance of the results.

Keywords: *Wireless Networks, Identity Attacks, Primary Keys, Attack Prevention.*

1. INTRODUCTION

As computing and networking are shifting from the static model of the wired Internet toward the new and exciting "anytime-anywhere" service model of the mobile Internet, wireless systems will become increasingly programmable, interfacing with converged devices, and supporting new mobile applications. One serious class of threats that will affect the successful deployment of mobile wireless technologies are spoofing attacks. Spoofing attacks can be launched with little effort. The reason stems from the shared nature of the wireless medium, where adversaries can perform passive monitoring of useful identity information and then masquerade as another device using the collected identity.

Spoofing attacks can facilitate a variety of advanced attacks to significantly impact the normal operation of wireless networks . Spoofing attacks on mobile wireless devices may further inflict security and privacy damages on the social life of the individual who carries wireless devices. There has been active work in detecting spoofing attacks. use of matching rules of Received Signal Strength (RSS) for spoofing detection, used cluster analysis of RSS, and modeled RSS readings as a Gaussian mixture model to capture antenna diversity. In this work, focus on spoofing attack detection in mobile wireless environments, that is, the wireless devices including the victim node and/or the spoofing node are moving around.

Most existing system detecting the spoofing attacks using cryptographic methods and cluster analysis methods. Cryptographic methods require the reliable key distribution and requirement management overhead. It is not always possible to detect the spoofing attacks. Attacks are detected based on the received signal strength(RSS).Cluster based analysis is performed by received signal strength. The clustering mechanism does not differentiate the RSS values calculated closely to each other. All those techniques are not accurately detect the spoofing attacks.

We focus on spoofing attack detection and localization. Works are related to [1],[4],[8]. Jie Yang Et al [1] determined the identity based attack used by received signal strength. D.Faria Et al [4] described detect the spoofing attacks using signal prints. Y chen Et al [8] describe the identity based attack detection using k means cluster algorithm.This method is performed based on the clustering formed. All those methods are not focusing the packet transmission path.In this work we are focusing the Packet transmission path as well as performing the following functions.

1)First one is Energy assumption and Path selection process. energy level is assumed in every node separately. Selecting the appropriate path for packet transmission. path is selected based on the transmission cost and delivery time.This process reduce the transmission cost and processing time.2) Node status: nodes are activated during transmission time. Activate which nodes is going to transmit the packets. remaining nodes are in sleep mode. By keeping sleep mode energy is conserved for packet transmission.3)primary key assignment: each network assigning the primary key for every node presented in their networks. Attackers are detected based on the primary key assignment. Attackers nodes are not contains the primary keys.4)data encryption: Packets are encrypted for secure packet transmission. Encryption avoid the view of the information presented in the packets from intermediate nodes.

In path selection process Select which is the best way for transferring data to destination node securely. After selection process is finished other paths are disabled and selected paths are enabled. Data is transferred in the selected path in secure manner. During data transfer the nodes are activated which node is going to transfer the data packets. Remaining nodes are in sleep mode. Sender nodes only active (i.e., Live Status) state mean while of all other nodes are inactive state (i.e., Sleep Status). After data transfer process is finished nodes are kept in sleep mode. In this way energy is conserved. Possibilities are minimized for attacker when nodes are in sleep mode. Multiple data packets are sending from one network to another one with encryption of hidden information will be passed. Attackers are easily detected and localized.

Security is provided in the selected path by performing data encryption for secure data transmission. Appropriate path selection process reduce the packet transmission time and cost is reduced. Intermediate attacker is detected. The network identifies the node location using received signal strength. Parent Network assigns primary key for all nodes. Parent network monitor the child network process.

Suppose source node in network2 sends packet to destination node in network3 means it directly sends packet to destination using node id. Because network 1(parent network) monitor the network2 and network3 (child networks). So packet don't go network 1. So routing path is minimized so it quickly sends data and time also minimized. The parent network assigns primary key for each node based on triangular shape connection with RSS. If the hacker enter in network2 means it didn't has primary key so parent network identify the hacker (spoofing attacks) easily. We demonstrate the experimental results in IEEE 802.11 network using network Simulator.

2. RELATED WORKS

The traditional methods to prevent the spoofing attacks is to use cluster base mechanisms and cryptographic based mechanisms [1],[3],[5],[6]. J.Yang et al [1] have introduced detection and localizing the spoofing attacks by using cluster based mechanisms based on the received signal strength cluster is formed. Based on the cluster formation the attacker is detected. It is not always possible to differentiate the RSS values for normal node and victim node. [3] J.Wu et al introduce a secure and efficient key management framework (SEKM). SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group.[5] A.Wool et al (2005) described to focus on the delay that the current initial authentication process introduces to an AP when a mobile STA is entering to an ESS for the first time as well as the delay in link establishment. Fast authentication is what mobile stations need in order to experience real mobile services. In this paper, we have presented an alternative solution for FIA, namely HIP-WPA which is based on HIP-DEX. [6] Y.Sheng et al implemented the MAC spoofing attacks in 802.11 networks exploit a fundamental vulnerability of the 802.11 protocol: the MAC addresses of wireless frames can be easily forged, imposing a serious security challenge. Physical-layer information, such as Received Signal Strength (RSS), is hard to forge arbitrarily and can be used to detect such spoofing.

Recently new approaches utilizing the primary keys assignments and packet ID validation for detecting Identity based attacks detection .In this paper assigning the primary keys for security purpose. Appropriate path is selected for reduce the transmission cost and time. Our works differs from previously described attack detection based on cryptographic and cluster mechanisms. None of existing work can detect the path for transmission time and cost reduction and always not possible to detect attacks. Our approach prevent the networks from attackers entry.

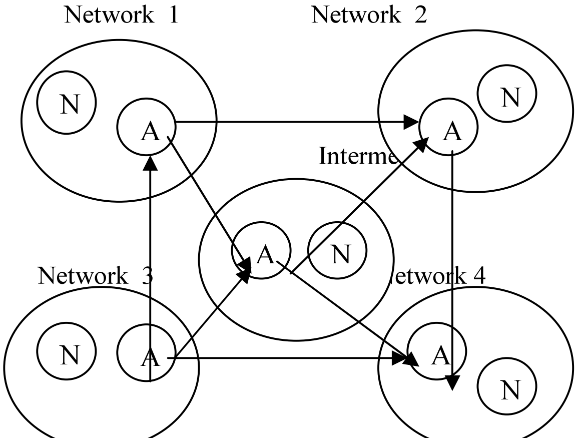
3. NODE ENERGY CONSUMPTION AND LOCALIZATION

To implement the Project concept, first we have to construct a network which consists of 'n' number of Nodes. The network assigns some energy level of each node. It also monitor the each node energy level. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. To show this concept we'll create the Node frame which contains the time. Based on the time change we can assume that the nodes are moving across the network. For each node we have to create a Node Frame which contains the Node information, Destination Node field to transfer the data.

Identify the current location of node by using received signal strength. Nodes are covered by data transmit distance. Because network monitor all the nodes information like Node Id, Password, energy level and other information , also server will monitor all the nodes communication. node id and passwords are registered before communication. These build the interconnection nodes for detecting the attacks as well as localize the positions of adversaries.

3. I Triangular Method:

Network will always be connected in the triangular method. Here which node send the data from its network then those network acts as the access point. Access point of the network will connect triangular shape of the network. So, access point network will monitor and maintaining the other 2 network details for avoid the spoofing attacks. Network cost will be low for maintaining thrice network at the access point of the same time by using triangular algorithm. It is used to identify the spoofing attacks in the network. Each network will be verifying the node ID on the data transmission with the Original ID Specified in the packet Header. If those two ID's are mismatch the available of spoofing nodes are detected easily. We conducted experiments using both an 802.11 (Wi-Fi) network and an 802.15.4(Zigbee) network.



Triangular Method

Nearest networks are connected with each other for packet transmission.If the network 1 is transmitting packet to network 3 means the intermediate network is also connected with network 1 & 3 details of those networks are updated with each other. updated network details are used to identify the attacker node in registered networks. packets are not possible to transmitted by the attackers even the attacker should know primary key value and node id for the reason that primary key is frequently changed and node id is previously registered in networks

Each network monitor the own nodes activity also. If the route is chosen from the source node of the packet delivery, then all the intermediate nodes in that path is act as live state from before sleep state. So, based on the minimal number of node with energy connectivity from Source node to destination node reaches then the best path will be selected. After selection of path other nodes are sleep.

4 FASTER RANDOMIZED ALGORITHM:

Primary key is assigned for created network nodes for attack detection . Parent Network assigns primary key for all nodes. Parent network monitor the child network process. Each network monitor the own nodes activity also. Attackers are detected by verifying the primary keys.It is a unique key not collaborate with other node keys. Source node assigns the primary key for packets during transmission. The assigned primary key dynamically changed with respect to one cycle completion. If attacker enter into the network to hack the packed information means does not encrypt the information because the primary key is changed.

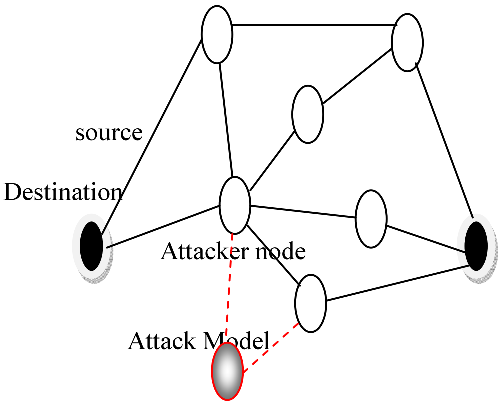
Primary key is assigned by using faster randomized algorithm. key is assigned for each node registered on the network. during the packet transmission the assigned primary key is changed with respect to one cycle. If the attacker is entered in the network the attacker within the networks are easily detected by primary key. Because the attacker does not have the primary key values.

4.1 Packet Encryption:

In packet encryption the transmitted content is converted.(i.e) plaintext to cipher text. Attacker are not able to view the original information. Data is transmitted from source node to destination node. We propose to use signcryption for encrypting the data. Signcryption performs both data encryption and digital signature generation. Encryption of packet requires primary key and digital signature from both source and destination. The attacker don't have the primary key when enter into the network so information encryption is restricted.

IV.II Attacker Detection:

Delivery of packets based on the received signal strength.RSS values varies with respect to location and transmission power levels. based on the Received signal strength , primary key and Id specified in the packet header attackers are detected. Created networks are connected in triangular shape. Each network act as server when it is l act as a source. The source network monitor the intermediate nodes and destination nodes. The node information like ID, password, energy and primary key is monitored. Based on the ID specified in the packet header the adversaries are easily detected.



IV.III Packet Delivery:

Best Route is chosen for successful packets delivery based on the time of delivery and cost. That means source choosing lot of path for delivering packet to destination based on energy level using RSS. Finally it identifies the best route for successful packets delivery based on time of delivery and cost. Energy level for nodes is reduced based on the packet transmission. Packets are transmitted in another path when the node energy level reached low energy level(i.e. >30J) for fast packet delivery.

5. PERFORMANCE EVALUATION:

Fig.1 presents energy level consumption. Networks assigns the energy level for each nodes. Level of the energy is reduced with respect to the packet size. In this proposed method we achieve the higher packet transmission and attacker detection by low energy level. Packets are transmitted in the selected path. Networks select the alternate path when the selected path nodes reached low energy (>30J).

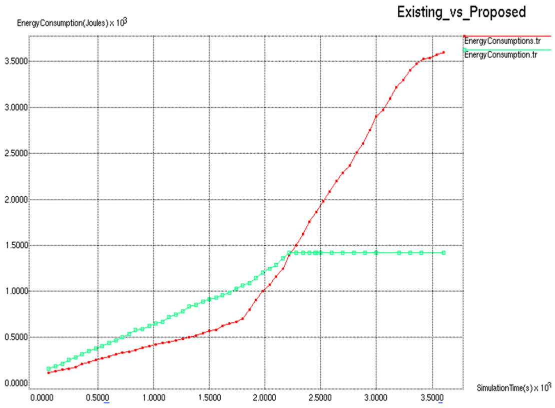


Fig. 1 Energy Level

The simulation result were carried out four networks. Three networks are connected in triangular shape. Information about all nodes presented within the networks are updated with each other networks. Networks 1,2 &3 are connected. Packets are transmitted within the networks 1,2 &3. The other networks are not possible to send or receive the packets. In this way the attackers are detected by received signal strength.Fig.2 presents the comparison between existing system and proposed works. Proposed method is highly effective in detecting and localizing the attackers with low energy level.

Attackers are localized by received signal strength and primary keys. Prevent data encryption from attacker by signcryption.

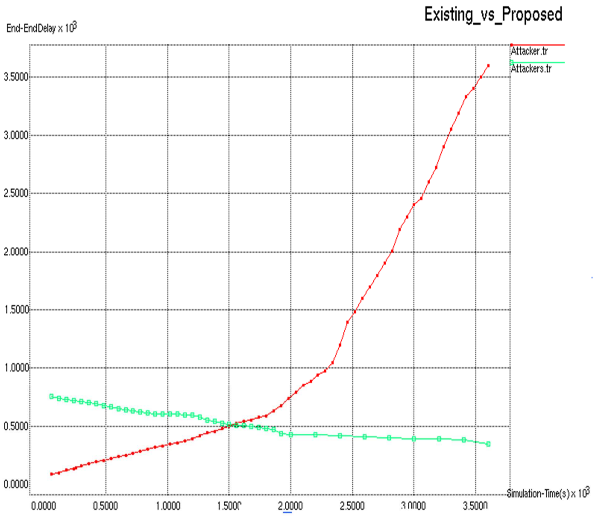


Fig.2 Attacker Detection

Detection and localization performance in existing work is much worse. Original node and fake nodes are not possible to clearly differentiated by using cluster based silence mechanism. In proposed work using primary key to achieve the higher detection and localization.

6. CONCLUSION:

In this work, we create a network and connected by using triangular method. In this method packets are transmitted securely. signcryption is used for security, both encryption and digital signature is performed. Determining the number of adversaries is particularly challenging problem. Based on the received signal strength the attackers is localized Prevent the packets from adversaries by assigned primary key values. Simulations based on NS-2 have been carried out to verify the performance of the proposed system. Experimental results illustrate that the proposed system outperforms all other multi spoofing schemes, including IEEE 802.11 distribution by the selective route mechanism in terms of the packet delivery, the standard end-to-end interruption, and the normalized routing overhead, false positive ratio.

REFERENCES:

[1] Jie Yang, Y.Chen, W.Trappe “Detection and localization of multiple spoofing attackers in wireless networks” proc. IEEE wireless networks, vol 24, jan 2013.

[2] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[3] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and Efficient Key Management in Mobile Ad Hoc Networks,” Proc. IEEE Int’l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[4] D. Faria and D. Cheriton, “Detecting Identity-Based Attacks in Wireless Networks Using Signalprints,” Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[5] A. Wool, “Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation,” ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength,”proc IEEE INFOCOM, Apr 2008.

[7] J. Yang, Y. Chen, and W. Trappe, “Detecting Spoofing Attacks in Mobile Wireless Environments,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.

[8] Y. Chen, W. Trappe, and R.P. Martin, “Detecting and Localizing Wireless Spoofing Attacks,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[9] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,” Proc. IEEE Int’l Conf. Comm. (ICC), pp. 4646-4651,June 2007.

[10] L. Sang and A. Arora, “Spatial Signatures for Lightweight Security in Wireless Sensor Networks,” Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.

[11] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

[12] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[13] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Sept. 2006.

[14] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.

[15] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

[16] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.

[17] K. Wang, "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data," Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China, 2007.