ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue Special 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Integrated Detection and Localization of Multiple Spoofing Attackers in WSN

[I]Manikandan.S, [II]Alangudi Balaji.N
[I]PG Scholar, Dept. of CSE, Sethu Institute of Technology, Virudhunagar, India
[II]Assistant Professor, Dept. of CSE, Sethu Institute of Technology, Virudhunagar, India

Abstract
Wireless spoofing attacks are occurs easily and reduce the networks performance. The node identity is verified by cryptographic authentication, due to requirements overhead conventional security approaches are not always suitable. In my paper, I propose to use spatial information, as the basis for detecting spoofing attacks, determining the number of attackers when multiple enemies masquerading as the same node identity and localizing more than one enemies. I propose to use the spatial correlation of received signal strength to detect the spoofing attacks. I then determine the number of attackers. I used Cluster-based mechanisms determine the number of attackers. The Support Vector Machines method used to increase the accuracy of determining the number of attackers. Integrated detection and localization system is used to localize the more than one attackers. I evaluated my techniques using the both an 802.11 network and an 802.15.4 network. When determining the number of attackers by using my method the result attain more than ninety percent hit rate. My localization results using algorithms provide high accuracy of localizing more than one enemies.

Keywords
Network Analysis, Spoofing Attack, Spoofing Detection, Localization, Wireless Network

I. Introduction

The wireless transmission medium can access by any user, so attackers can easily access any transmission. Adversaries can easily buys a low cost wireless devices and launch a variety of attacks by using these available platforms. There are various types of attacks, from these attacks the identity based spoofing attack are said to be easy to launch and cause a serious damages to the network.In the identity based spoofing attack attackers use the same identity to transfer the data. So I propose to use spatial information, for detecting the spoofing attacks, determining the number of attackers when multiple enemies masquerading as the same node identity and localizing more than one enemies.. I propose to use the spatial correlation of received signal strength to detect the spoofing attacks. I then determine the number of attackers. I used Cluster-based mechanisms determine the number of attackers.The Support Vector Machines method used to increase the accuracy of determining the number of attackers.Integrated detection and localization system is used to localize the more than one attackers.

To use the received signal strength based spatial correlation, a physical property present in the wireless node that is difficult to falsify and they are not depends on cryptography for detecting spoofing attacks. I concerned with attackers, they have different locations than legitimate wireless nodes, and a spatial information is used to detect spoofing attacks that has a power to not only detect the presence of the attacks but also localize the attackers.

In the existing system the cryptographic method needs reliable key distribution, management, and maintenance. It is not always possible to apply these methods because of its infrastructural and management overhead. In the existing system, cryptographic method node are said to be easily attacked, which is a serious matter. The wireless nodes are said to be easily accessible, by allowing their memory. The memory is said to be scanned by the attackers. Cryptographic method only protect the data frames.In the proposed system, to detect the attacks on wireless localization, proposed to use the direction of arrived and received signal strength of the signals to localize adversaries. In my work, I choose a group of algorithms based on RSS to perform the work of localizing more than one attackers and calculate the performance in the terms accuracy of localization.

II. Related Work

In the existing system the cryptographic method needs reliable key distribution, management, and maintenance. It is not always possible to apply these methods because of its infrastructural and management overhead. In the existing system, cryptographic method node are said to be easily attacked, which is a serious matter. The wireless nodes are said to be easily accessible, by allowing their memory. The memory is said to be scanned by the attackers. Cryptographic method only protect the data frames.

F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," 2004. From this paper I identified the Spoofing attacks can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, access point (AP) attacks, and eventually Denial-of-Service (DoS) attacks. In this they describe possible denial of service attacks to infrastructure wireless 802.11 networks. The results show that serious vulnerabilities exist in different access points can easily hinder any legitimate communication within a basic service set.

D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints", Sept. 2006. From this paper I found a broad survey of possible spoofing attacks, such as network resource utilization attack and denial-of-service attack. Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client. In this paper a transmitting device can be robustly identified by its signal print. Signal prints can be defeated, such as by the use of multiple synchronized direction antennas, these situations present a challenge for an intruder.

B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," 2005. From this paper I found a most existing approaches to address potential spoofing attacks employ cryptographic schemes and the disadvantages of cryptographic schemes. They propose a secure and efficient key management (SEKM) framework for mobile adhoc network. SEKM builds a public key infrastructure (PKI) by applying a secret sharing scheme. In fact any cryptographic means

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

is ineffective if its key management is weak. Key management is also a central aspect for security in the mobile adhoc network. P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF-Based User Location and Tracking System," 2000. From this paper I identified that using RSS is an attractive approach because it can reuse the existing wireless infrastructure and is highly correlated with physical locations. Dealing with ranging methodology, range-based algorithms involve distance estimation to landmarks using the measurement of various physical properties such as RSS.

III. Proposed System

In the proposed system, to detect the attacks on wireless localization, proposed to use the direction of arrived and received signal strength of the signals to localize adversaries. In my work, I choose a group of algorithms based on RSS to perform the work of localizing more than one attackers. The Proposed system can be moduled as following.

- Network Analysis
- Spoofing Attack
- Attack Detection
- Localization

A. Network Analysis

The proposed system is initiatedwith a fixed-length walk from the node. This walk should be long enough to ensure that the visited peers represent a close sample from the underlying stationary distribution. I then retrieve certain information from the visited peers, such as the system details and process details. It acting as source for the network .In sender used to create sends the request and received the response and destination used to receive the request and send the response for the source.

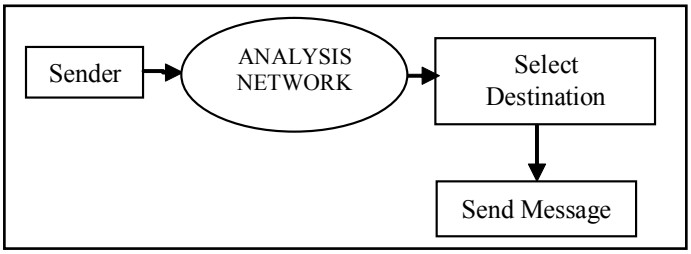

Fig. 1: Network Analysis

B. Spoofing Attacks

Spoofing attacks are easy to launch and can cause damage to the performance of a network. In an 802.11 network, it is easy for an attacker to collect a MAC address during passive monitoring and then attacker modify the MAC address by simply issuing an If config command to masquerade as another device. In the proposed system the frames like data, management, control are said to be protected. In the existing security techniques like Wired Equivalent Privacy, WiFi Protected Access, or 802.11i, such techniques can only protect the data frames, an attacker can spoof management or control frames to cause impact on networks.

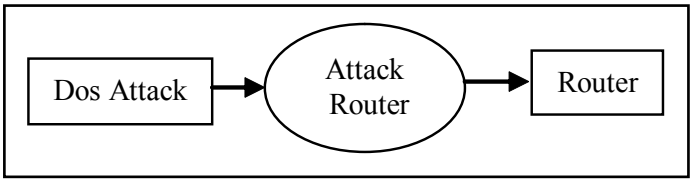

Fig. 2: Spoofing Attack

C. Attack Detection

In the attack detection instead of cryptographic based method, My work is new because none of the existing work can determine the number of attackers when there are more than one enemies masquerading as the same identity. The spatial correlation of RSS is used to detect the attack. The cluster based mechanism is used to detect the number of attackers. This mechanism is said to be improved by the support vector machine. That is the SVM is used to improve the accuracy of determining the number of attackers.

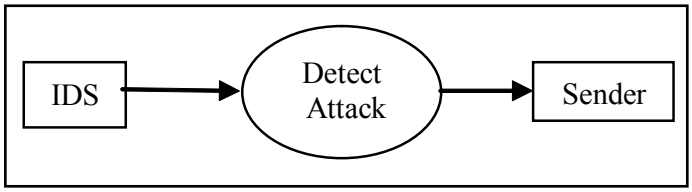

Fig. 3: Attack Detection

D. Localization

The proposed approach can correctly localize more than one enemies even the transmission power levels of the attackers varies. Algorithm used for a localization are area based probability and RADAR gridded algorithms. Localization estimation using RSS which are about 15 feet. When the nodes are less than 15 feet apart, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90 percent, but still greater than 70 percent. When spoof moves closer to the attacker also increases the probability to expose itself, now the detection rate goes to 100 percent. When the spoofing node is about 45-50 feet away from the original node. The detection rate is said to be lesser.

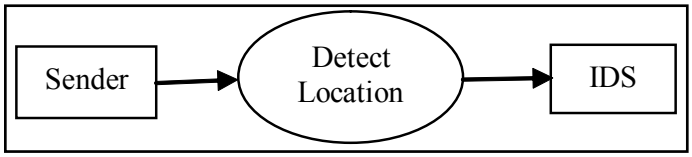

Fig. 4: Localization

IV. Performance Evaluation

This graph shows the packet delivery ratio. The packet delivery ratio graph consist of time as X axis and delivery ratio as a Y axis. In existing system, when the time is increases the delivery ratio is said to be reduces. In the proposed system, when the time is increases the delivery ratio is also said to be increases. So in the proposed system the delivery of the packet is said to be faster and higher than the existing system.

Fig. 5: Packet Delivery Ratio

This graph shows the security performance. The security graph consist of time as X axis and security value as a Y axis. In existing system, when the time increases the security is said to be decreases. In the proposed system, when the time increases the security is also said to be increases. So in proposed system the data is said to be well secured than the existing system.

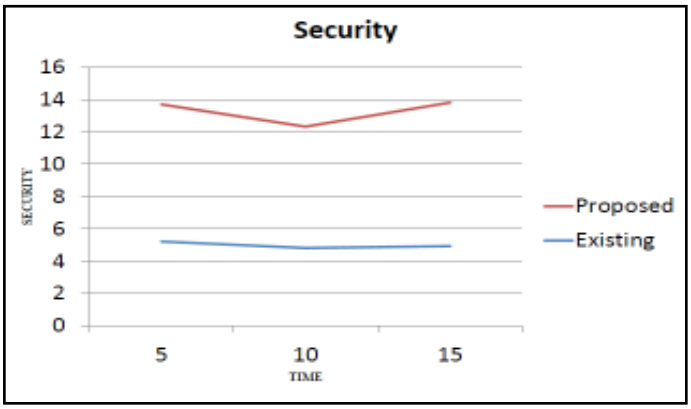

Fig. 6: Security

This graph shows the throughput performance. The throughput graph consist of time as X axis and throughput value as a Y axis. In existing system, when the time increases the throughput is said to be decreases. In the proposed system, when the time increases the throughput is also said to be increases. So in proposed system the throughput is said to be higher than the existing system.

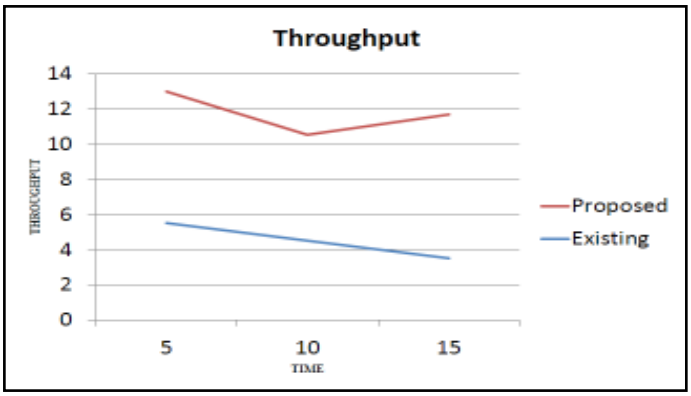

Fig. 7: Throughput

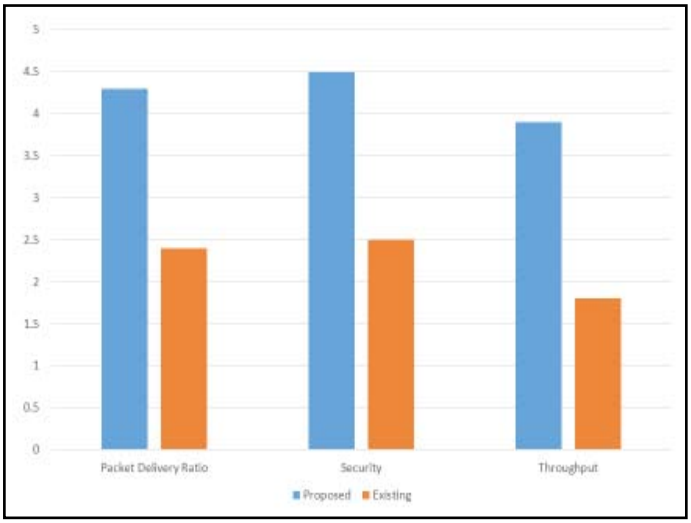

Fig. 8: Comparison between Proposed and Existing System

Table 1: Comparison between Proposed and Existing System

Systems	Packet Delivery	Security	Throughput	Hit Rate
Proposed	54.5	75.3	70.9	95
Existing	30.3	31.5	35.8	70

V. Conclusion

In my work, I used a RSS based spatial correlation, a physical property presented with the wireless device that is said to be difficult to falsify and they are not depends on the cryptography method for attacks detection in WSN. For attack detection I proposed an analysis of using the spatial correlation of Received Signal Strength. I evaluate the test depends on the cluster analysis of Received Signal Strength. I can detect attacks, the number of enemies and I can localize any number of attackers even in different transmission levels and remove the attackers using my approach integrated detection and localization of multiple spoofing attackers in WSN.

VI. Future Work

In the future the integrated detection and localization system can detect the attackers, calculate the number of attackers and localizing any number of enemies in different transmission levels by using the hash key algorithm. This algorithm is used to generate the hash key. The hash key is used for both the encryption and decryption. The performance of this algorithm achieves higher results, and it provide effective result in detecting the attacks, calculating the number of attackers and localizing enemies.

VII. Acknowlegement

References

[1] *F. Ferreri, M. Bernaschi, and L. Valcamonici "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2004.*

[2] *D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 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] *P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF- Based User Location andTracking System," Proc. IEEE INFOCOM, 2000.*

[5] *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*

[6] *M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.*

[7] *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.*

[8] *V.Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[9] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.
[10] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.
[11] 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.
[12] 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.
[13] 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.
[14] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.
[15] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

Author's Profile and Image

S.Manikandan received the Bachelor of Technology degree in Information Technology from Anna University, Chennai. And currently doing a Master of Engineering degree in Computer Science and Engineering in Sethu Institute of Technology, under the control of Anna University Chennai. My area of interest includes networking.

Mr.N.Alangudi Balajireceived the M.Tech degree in Information Technology and doing PhD Degree. He is currently working as an Assistant Professor in Department of Computer Science and Engineering at Sethu Institute of Technology.His area of interest includes networks and embedded systems.