Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.230 – 239

RESEARCH ARTICLE

RECOGNIZING AND DISCOVERING SPOOFING ATTACKS FOR MOBILE ADHOC NETWORK

T.Navaneethan[1], M.Lalli[2]

[1] School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli- 620023, India

[2]School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli- 620023, India

[1] navaneethanvel@gmail.com, [2] lalli_gss@yahoo.co.in

Abstract - Wireless networks are exposed to many attacks which of one is spoofing attack. The networks performance will be affected more when the attackers are present. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. K means clustering is used to determine the number of attackers. In this paper we proposed to use Enhanced Sequential Probability Ratio test (ESPRT) technique. This is the fast and effective technique to detect the mobile replica nodes. The network is divided into set of zones, and then trust level is established for each zone to detect untrustworthy zones. The entire zone is considered as untrustworthy if trust level goes below trust threshold. The base station will revoke the zone if it considers the zone as untrustworthy. The main benefit of this zone-based detection approach lies in achieving fast node compromise detection and revocation while saving the large amount of time and effort.

Keywords: MANET, Spoofing, Security, Zone based, Mobile Replica Node

I. Introduction

MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad hoc network is self organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. The set of

© 2014, IJCSMC All Rights Reserved

applications for MANETs is diverse, ranging from large scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Security solutions are important issues for MANET, especially for those selecting sensitive applications, have to meet the following design goals while addressing the above challenges. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to security attacks.

II. Related Work

Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

In this study [1], use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Then it formulates the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, it explores using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, it developed an integrated detection and localization system that can localize the positions of multiple attackers.

Access Points Vulnerabilities to Dos Attacks in 802.11 Networks

In this paper [2], it describes possible denial of service attacks to infrastructure wireless 802.11 networks. To carry out such attacks only commodity hardware and software components are required. The results show that serious vulnerabilities exist in different access points and that a single malicious station can easily hinder any legitimate communication within basic service set. The peculiar features of wireless networks suggest a greater exposure to Denial of Service (DoS) attacks than wired networks. Since the wireless medium does not have well defined physical bounds, a malicious station can appear in the range of such a network and launch an attack in order to stop any legitimate communication.

The aim of this paper is to investigate how these kinds of attacks can be carried out. In particular it tried to identify some simple attack schemes that might lead to a DoS effect and then observed the reactions of various types of infrastructure networks to these attacks.

Detecting Identity-Based Attacks in Wireless Networks Using Signalprints

In this paper [3], wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities. We can see that, different from MAC addresses or other packet contents, attackers do not have as much control regarding the signal prints they produce. Moreover, using measurements in a test bed network, we demonstrate that signal prints are strongly correlated with the physical location of clients, with similar values found mostly in close proximity. By tagging suspicious packets with their corresponding signalprints, the network is able to robustly identify each transmitter independently of packet contents, allowing detection of a large class of identity-based attacks with high probability. After a client authenticates successfully and session keys are used to encrypt and authenticate packets sent over wireless links, the network can securely verify if the source MAC address in a packet is correct. Without this mechanism, however, wireless installations have to rely solely on MAC addresses for client identification: two devices in a network using the same address are treated as a single client, even if they generate conflicting or inconsistent requests.

Detecting 802.11 Mac Layer Spoofing Using Received Signal Strength

In this paper [4] assuming the attacker and the victim are separated by a reasonable distance, RSS can be used to differentiate them to detect MAC spoofing, as recently proposed by several researchers. By analyzing the RSS pattern of typical 802.11 transmitters in a 3-floor building covered by 20 air monitors, we observed that the RSS readings followed a mixture of multiple Gaussian distributions.

They are discovered that this phenomenon was mainly due to antenna diversity, a widely-adopted technique to improve the stability and robustness of wireless connectivity. This observation renders existing approaches ineffective because they assume a single RSS source.

We propose an approach based on Gaussian mixture models, building RSS profiles for spoofing detection. Experiments on the same tested show that our method is robust against antenna diversity and significantly outperforms existing approaches. At a 3% false positive rate, we detect 73.4%, 89.6% and 97.8% of attacks using the three proposed algorithms, based on local statistics of a single AM, combining local results from AMS and global multi-AM detection, respectively.

Sequence Number-Based Mac Addresses Spoof Detection

In this paper [5], the exponential growth in the deployment of IEEE 802.11-based wireless LAN (WLAN) in enterprises and homes makes WLAN an attractive target for attackers. Attacks that exploit vulnerabilities at the IP layer or above can b e readily addressed by intrusion detection systems designed for wired networks. However, attacks exploiting link-layer protocol vulnerabilities require different set of intrusion detection mechanism. Most link-layer attacks in WLANs are denial of service at-tacks and work by spoofing either access points (APs) or wireless stations.

Spoofing is possible because the IEEE 802.11 standard does not provide per frame source authentication, but can b e effectively prevented if a proper authentication is added into the standard. Unfortunately, it is unlikely that commercial WLANs will supp ort link-layer source authentication that covers both management and control frames in the near future. Even if it is available in next-generation WLANs equipments, it cannot protect the large installed base of legacy WLAN devices.

This paper proposes an algorithm to detect spoofing by leveraging the sequence number field in the link-layer header of IEEE 802.11 frames, and demonstrates how it can detect various spoofing without modifying the APs or wireless stations. The false positive rate of the proposed algorithm is zero, and the false negative rate is close to zero. In the worst case, the proposed algorithm can detect a spoofing activity, even though it can only detect some but not all spoofed frames.

III. PROPOSED WORK

The proposed system work is motivated from mitigating the limitations of previous schemes. In particular, the new system proposes a method in which the nodes are fixed as well as in movement. A reputation-based trust management scheme is designed to facilitate fast detection of compromised nodes. The key idea of the scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised.

Specifically, first divides the network into a set of zones, establish trust levels for each zone, and detect untrustworthy zones by using the Sequential Probability Ratio Test (ESPRT). The ESPRT decides a zone to be untrustworthy if the zone’s trust is continuously maintained at low level or is quite often changed from high level to low level. Once a zone is determined to be untrustworthy, the base station or the network operator performs software attestation against all nodes in the untrustworthy zone, detects compromised nodes with subverted software modules, and physically revokes them.

In addition, a novel mobile replica detection scheme is proposed based on the Sequential Probability Ratio Test (ESPRT). The new system uses the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, a benign mobile sensor node’s measured speed will nearly always be less than the system-configured maximum speed as long as it employs a speed measurement system with a low error rate. On the other hand, replica nodes are in two or more places at the same time. This makes it appear as if the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes’ measured speeds will often be over the system-configured maximum speed.

Enhanced Sequential Probability Ratio Test

The Enhanced Sequential Probability Ratio Test (ESPRT) which is a statistical hypothesis testing. ESPRT has been proven to be the best mechanism in terms of the average number of observations that are required to reach a decision among all sequential and non-sequential test processes. ESPRT can be thought of as one dimensional random walk with lower and upper limits.

Before the random walk starts, null and alternate hypotheses are defined in such a way that the null one is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation.

The main idea of the proposed scheme is to use sequential hypothesis testing to detect suspect regions in which compromised nodes are likely placed. In these suspect regions, nodes perform software attestation, leading to the detection and revocation of the compromised nodes. Through analysis and simulation, it is shown that the proposed scheme provides effective and robust compromised sensor node detection capability with little overhead.

A reputation-based trust management scheme is designed to facilitate fast detection and revocation of compromised nodes. The key idea of the scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised. In addition, a fast and effective mobile replica node detection scheme is proposed using the Sequential Probability Ratio Test. To the best of the knowledge, this is the first work to tackle the problem of replica node attacks in mobile sensor networks. Specifically, it first divide the network into a set of zones; establish trust levels for each zone, and detect untrust worthy zones by using the Sequential Probability Ratio Test (ESPRT).

The ESPRT decides a zone to be untrustworthy if the zones trust is continuously maintained at low level or is quite often changed from high level to low level. Once a zone is determined to be untrustworthy, the network operator performs software attestation against all nodes in the untrustworthy zone, detects compromised nodes with subverted software modules, and physically revokes them.

A straight forward approach for untrustworthy zone detection is to decide a zone as untrustworthy by observing single evidence that its trust value is less than a trust threshold. However, this approach does not consider the zone trust measurement error. Due to the errors in the zone trust measurement, a trustworthy zone could be detected a sun trustworthy. To minimize the false positives and false negatives, it needs to make a decision with multiple pieces of evidence rather than single evidence. To satisfy this requirement, it applies the ESPRT to node compromise detection and revocation problem.

It believe that the ESPRT is well-suited for tackling untrustworthy zone detection problem in the sense that can construct a random walk with two limits in such a way that each walk is determined by the trust value of a zone. Indeed, the lower and upper limits are properly configured to be associated with the excess and short fall of a trust threshold, respectively. Specifically, every sensor node in a zone acts as trust aggregator in a round-robin manner. In each timeslot, the trust aggregator computes a trust level for its zone and reports the zone’s trust level to the base station.

The base station performs the ESPRT with zone trust information. Each time a zone’s trust is below a trust threshold, it will expedite the test process to accept the alternate hypothesis that a zone is untrustworthy. Once the base station decides that a zone is untrustworthy, the network operator performs software attestations against all sensor nodes to detect and revoke the compromised nodes in the zone. The main benefit of this zone-based detection approach lies in achieving fast node compromise detection and revocation while saving the large amount of time and effort that would be incurred from using periodic software attestation. By detecting an entire zone at once, the

© 2014, IJCSMC All Rights Reserved

system can identify the approximate source of bad behavior and react quickly, rather than waiting for a specific node to be identified.

Also, when multiple nodes are compromised in one zone, they can all be detected and revoked at one time. Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/or putting new data or controls on that node.

Algorithm process for enhanced ESPRT:

```
DECLARATION: $n$=0,$w_n$=0
INPUT: location information $L$ and time information $T$
OUTPUT: accept the hypothesis $H_0$ or $H_1$
curr_loc=$L$
curr_time=$T$
if $n$>0 then
    compute $T_0(n)$ and $T_1(n)$
    compute speed 0 from curr_loc and prev_loc, curr_time and prev_time
    if 0>$V_{max}$ then
        $w_n$=$w_n$+1
    end if
    if $w_n$>=$T_1(n)$ then
    Accepts the hypothesis $h_1$ and terminate the test
    end if
    if $w_n$<=$T_0(n)$ then
        initialize $n$ and $w_n$ to  0 and accepts the hypothesis $H_0$
    return;
    end if
end if
$n$=$n$+1
prev_loc=curr_loc
prev_time=curr_time
```

ALGORITHM STEPS

1) Create a network of ‘n’ nodes and save the information in the database table.
2) Draw the network with the available node information.
3) Random walk procedure is worked out so that the nodes’ mobility is carried out by just moving its location with ‘n’ pixels below (the given speed) in both x and y direction. For example, if the speed is given as 10 units, then a random value below 10 is chosen, and the node is moved in x or y direction.

This is carried out for all nodes. For simulation, the timer is set to 5 seconds. So once each 5 seconds, all the nodes are moved within the given speed horizontally or vertically.

4) The nodes are sending their location to their neighbor nodes. The node is treated as neighbor to one, if it is within the given pixel units. For example, the unit is given as 50, then a node with left position in the space with 150 x value and another node with 180 x value is treated as neighbor nodes. This is applicable to y axis also. So in the rectangular area of 50 units (side), when the two nodes fall inside, then they are treated as neighbor nodes.

5) The nodes are updating their location information once in 10 seconds. The arrow lines are drawn during the animation such that from all nodes, the line is drawn to the base station. The area located at left bottom corner of the drawing space in the form.

6) Replica Attack: When a button is clicked, a node is chosen randomly which behaves as attacker node; a node is chosen randomly which behaves as affected node. The attacker node through sends the current location information, it sends its id as the affected node. So the base station receives updates with two ids at single update. Now, the base station needs to identify which node is correct and which is attacker.

7) If two nodes send same id, then the base station, collects the previous location information of the same id. Any one of the entry will have wrong previous location. At the same time, the neighbor nodes location data is also used such that, the affected nodes neighbors update correct location of suspected id whether the attacker nodes neighbor nodes update wrong location and the attacker node will be identified.

8) Then the node is revoked from the network.

IV. IMPLEMENTATION

The following **Table 1**describes experimental result for existing system error rate analysis. The table contains zone id, time interval (per sec), node id, affect number of node id details and error rate percentage details are shown

Zone ID	**Times (sec)**	**Node ID**	**Total No. of. Attacker Node**	**Error Rate (%)**
1	**60**	N0	**45**	**75.00**
1	**120**	N4	**43**	**71.66**
1	**180**	N18	**26**	**43.33**
1	**240**	N1	**22**	**36.66**
1	**300**	N7	**20**	**33.33**
1	**360**	N19	**18**	**30.00**

© 2014, IJCSMC All Rights Reserved

1	**420**	N15	**11**	**18.33**
1	**480**	N9	**5**	**8.33**
1	**520**	N20	**4**	**6.66**
1	**580**	N11	**3**	**5.00**

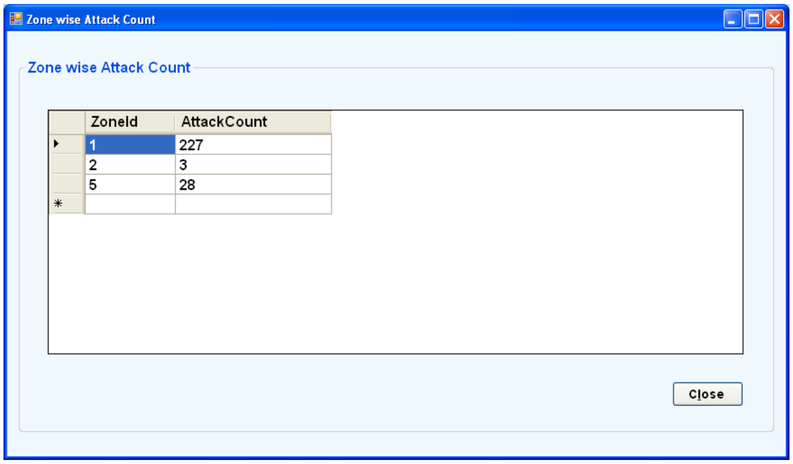
Table 1 Performances Result for Existing System

The following **Table 2** describes experimental result for proposed system error rate analysis. The table contains zone id, time interval (per sec), node id, affect number of node id details and error rate percentage details are shown

Number of Zone ID	**Times (sec)**	**Node ID**	**Total No. of. Attacker Node**	**Error Rate (%)**
1	**60**	N0	**52**	**86.66**
1	**120**	N4	**51**	**85.00**
2	**180**	N18	**32**	**53.33**
1	**240**	N1	**28**	**46.66**
1	**300**	N7	**25**	**41.66**
2	**360**	N19	**24**	**40.00**
5	**420**	N15	**13**	**21.66**
5	**480**	N9	**8**	**13.33**
5	**520**	N20	**6**	**10.00**
1	**580**	N11	**5**	**8.33**

Table 2 Performances Result for Proposed System

The following **Figure 1** describes experimental result for proposed system affect zone wise attacker node count analysis. The figure contains affect number of node id details and affect zone id count details are shown



ZoneId	AttackCount
1	227
2	3
5	28

Figure 1 Experimental Zone wise Attacker count in Proposed System

The following graph **Figure 2** show the hit rate comparison for the existing work and for the proposed work.

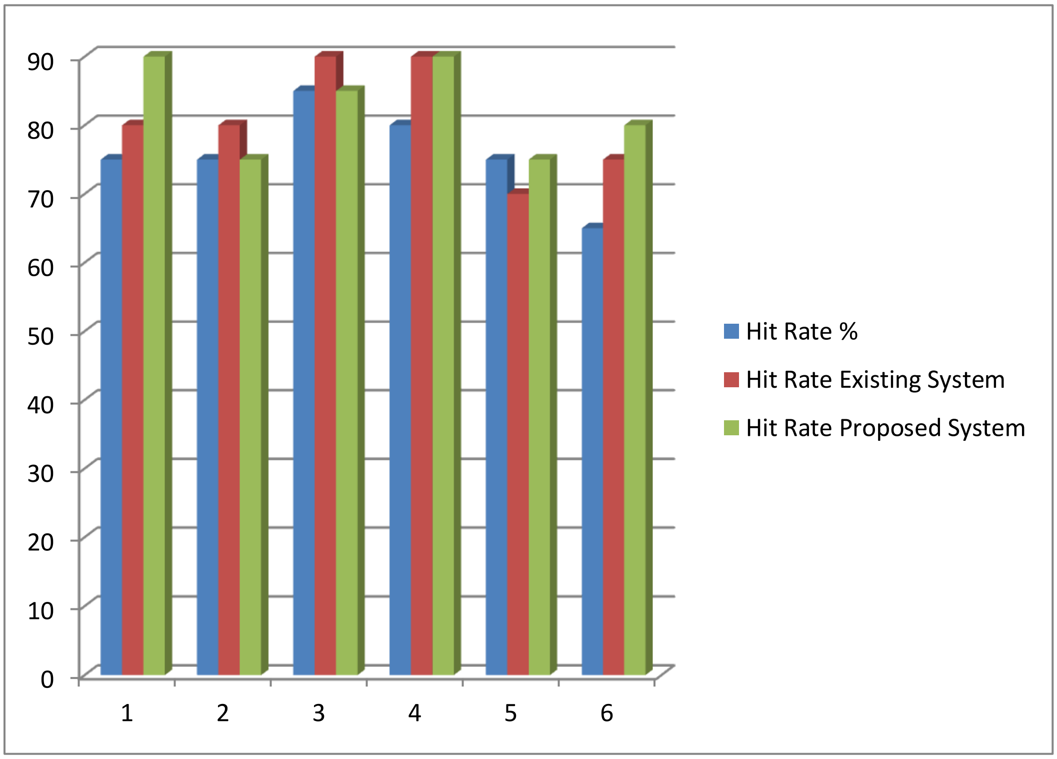


Figure 2 Hit rate Comparisons

V. CONCLUSION

This paper uses received signal strength-based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. It provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. The approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. In addition, a zone-based node compromise detection scheme is proposed using the Enhanced Sequential Probability Ratio Test (ESPRT). Furthermore, several possible attacks are described against the proposed scheme and proposed counter-measures against these attacks. The scheme is evaluated in simulation under various scenarios. The experimental results show that the scheme quickly detects untrustworthy zones with a small number of zone-trust reports.

REFERENCES

[1] Jie Yang,Yingying chen, Wade Trappe and Jerry Cheng **"Detection and Localization of Multiple Spoofing Attackers in Wireless Networks"** (January-2013).

[2] 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.

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

[4] J. Sheng, K. Tan, G.Chen, D.Kotz and A. Campbell **"Detecting 802.11 Mac Layer Spoofing Using Received Signal Strength",** Proc of Google. Inc at Dartmouth ISTS.

[5] 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.

[6] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book **The Handbook of Ad Hoc Wireless Networks (chapter 1)** CRC Press LLC, 2003.

[7] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book **The Handbook of Ad Hoc Wireless Networks ,(chapter 30)** CRC Press LLC, 2003.

[8] J. Bellardo and S. Savage, **"802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,"** Proc. USENIX Security Symp., pp. 15-28, 2003.

[9] 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.

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