IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 10, October 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Physical Layer Security In Wireless Local Area Network

[1]R.Divya, [2]K.Ravikumar

[1]Research Scholar, Dept. of Computer Science, Tamil University, Thanjavur-613010.

[2]Asst.Professor, Dept. of Computer Science, Tamil University, Thanjavur, -613010.

ABSTRACT

Wireless sensor network protocols, such as routing, time synchronization or data aggregation protocols make use of collaborative techniques to minimize the consumption of scarce resources in sensors. However, compromised and misbehaving nodes are a serious threat, as an attacker can employ them to eavesdrop on communication, inject forged data, or manipulate protocol operation. In this context, Wireless revocation protocols play a decisive role since they allow removing compromised nodes in an efficient way. The design of Wireless revocation protocols is challenging due to technical restrictions of sensor nodes, the Wireless operation of sensor networks, and the presence of compromised nodes that can collude to subvert protocol operation. We propose the secrecy rate maximization security protocol (SRM) to enhance network security and enable efficient Wireless revocation. The SRM is based on the distribution of revocation information - so called partial revocation votes - to the neighbors of a node as prerequisite to join the network. If an intruder refuses to disclose its revocation votes, the network does not allow it to join. Thus, the node is prevented from attacking the network. If the intruder cooperates by disclosing its revocation information, it can endanger the network neither, since its neighbors, which cooperate to monitor its correct operation, can use the revocation information to ban it from the network.

Keywords: Attacks, Network Performs , Attackers Performs, Data Communication.

I.INTRODUCTION

Wireless networks have become an indispensable part of our daily life, widely used in civilian and military applications. Security is a critical issue in wireless applications when people rely heavily on wireless networks for transmission of important/private information, such as credit card transactions or banking related data communications. Therefore, the ability to share secret information reliably in the presence of adversaries is extremely important. Adversaries may attempt to launch various attacks to gain unauthorized access to and modify the information, or even disrupt the information flows.

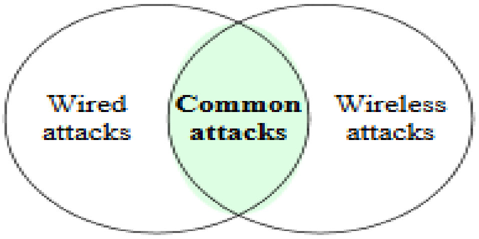
The authors in extended their previous work by considering the presence of imperfect CSI. Based on an information-theoretic formulation of the problem, in which two legitimate partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent channel, the important role of fading was characterized in terms of the average secure communication rates and outage probability. The authors in developed a secure communication protocol that adopts the following four-step procedure to ensure wireless information-theoretic security:

- Common randomness via opportunistic transmission
- Message reconciliation
- Common key generation via privacy amplification
- Message protection with a secret key

It was suggested in that perfect secrecy is achievable using physical layer techniques subject to the condition that the channels are unknown to unauthorized users or the channel of the unauthorized users is noisier than that of the authorized users.

EXISTING SYSTEM

Providing a secure system can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on wireless networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not.



(i)**Passive Attacks:**

In passive attacks, an intruder snoops the data exchanged without altering it. The attacker does not modify the data and does not inject additional traffic. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attacks are difficult to detect. Powerful encryption

(ii)**Active Attacks**

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. An attacker can create an active attack by modifying packets or by introducing false information in the ad hoc wireless network. Active attacks can be divided into internal and external attacks:

•Internal Attacks are from compromise nodes that were once legitimate part of the network. Since the adversaries are already part of the network as authorized nodes, they are much more severe and difficult to detect when compared to external attacks.

•External attacks are carried by nodes that are not legitimate part of the network. Such attacks can be prevented by using encryption, firewalls and authentication. Many attacks have been identified in literature on WLANs.

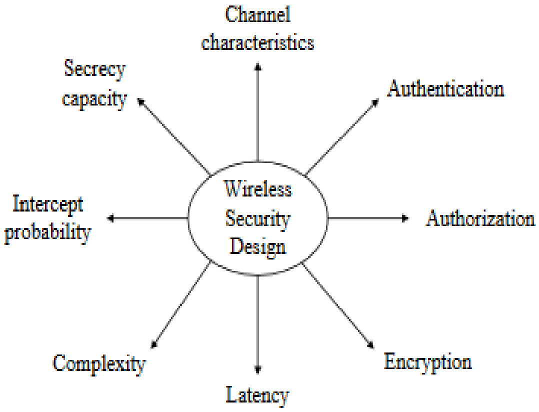
Advantage:

Confidentiality:

Confidentiality ensures that the data/information transmitted over the network is not disclosed to unauthorized users.

Disadvantage:

- If the authentication server authorizes the client, then the client is allowed to access the LAN.
- The AP switches the client’s port to authorized state and the client is allowed to resume normal network transactions.



II.PROPOSED SYSTEM:

Providing the network security is an important objective in the design and implementation of WLANs. Communication in wireless network is broadcast by nature and therefore all devices within the communication range of the sender receive the transmission. Thus, it becomes critical to protect data and other resources from unauthorized users. Infrastructure based WLANs assume the use of an AP that dictates the access to the wireless medium. For infrastructure based WLAN, it becomes critical to assure that only authorized users connect to the network, to keep user credentials from being hijacked during authentication, and to assure the privacy of the data being transmitted between the client and the AP. and implement sink attack and warm hole attack .

Confidentiality can be achieved by using different encryption techniques such that only legitimate users can analyse and understand the transmission.

Authentication:

The function of the authentication service is to verify a user's identity and to assure the recipient that the message is from the source that it claims to be from.

Access Control:

This service limits and controls the access of a resource such as a host system or application. To achieve this, a user trying to gain access to the resource is first identified (authenticated) and then the corresponding access rights are granted.

Integrity Control:

The function of the integrity control is to assure that the data received are exactly as sent by an authorized party. That is, the data received contain no modification, insertion, deletion, or replay.

III.MODULES

- Inside (sink hole attack)
- Outside(warm hole attack)
- Network performance
- Attacker performance
- Data Communication

Inside (sink hole attack)

One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information.

Sinkhole attack is an insider attack were an intruder compromise a node inside the network and launches an attack. Then the compromise node try to attract all the traffic from neigh bore nodes based on the routing metric that used in routing protocol.

Outside (warm hole attack)

The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally. The wormhole attack is one of the most severe security attacks in wireless ad hoc networks. In this paper, we analyse the effect of the wormhole attack in shortest path routing protocols. Using analytical and simulation results, we show that a strategic placement of the wormhole can disrupt on average 32% of all communications across the network.

Network formation

Network formation is an aspect of network science that seeks to model how a network evolves by identifying which factors affect its structure and how these mechanisms operate.

Attacker performance

In computer and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an Asset.

Types of attack

An attack can be active or passive.

- An "active attack" attempts to alter system resources or affect their operation.
- A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., wiretapping.)

An attack can be perpetrated by an insider or from outside the organization; An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Data communication

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data.

IV. CONCLUSION

Physical layer security has recently become an emerging technique to complement and significantly improve the communication security of wireless networks. Compared to cryptographic approaches, physical layer security is a fundamentally different paradigm where secrecy is achieved by exploiting the physical layer properties of the communication system, such as thermal noise, interference, and the time-varying nature of fading channels. . Wireless networks have become an indispensable part of our daily life, widely used in civilian and military applications. Security is a critical issue in wireless applications when people rely heavily on wireless networks for transmission of important/private information, such as credit card transactions or banking related data communications. Therefore, the ability to share secret information reliably in the presence of adversaries is extremely important. Specifically, the proposed cooperative transmission is replaced by a cooperative jamming (CJ)scheme if either security. Written by pioneering researchers, **Physical Layer Security in Wireless Communications** supplies a systematic overview of the basic concepts, recent advancements, and open issues in providing communication security at the physical layer. It introduces the key concepts, design issues, and solutions to physical layer security in single-user and multi-user communication systems, as well as large-scale wireless networks.

V. FUTURE ENHANCEMENT

This work had implemented an Energy efficient Channel Adaptive MAC protocol in a wireless sensor network with static nodes. This scheme had provided improvement gains in Energy efficiency, Throughput, Delay, Bandwidth and Delivery Ratio. Wireless ad hoc networks of battery powered micro sensors are proliferating rapidly and transforming the way information is gathered, processed and communicated. These networks are envisioned to have hundreds of inexpensive sensors with sensing, data processing and communication components. They typically operate in unattended mode, communicate over short distances and use multi hop communication. Many challenges are introduced due to the limited energy, large number of sensors, unfriendly working environment and nature of unpredictable deployment of the sensor network. Energy conservation is found to be the foremost among them since it is often cost prohibitive or infeasible to replenish the energy of the sensors.

REFERENCES:

[1] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, “Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming,” in Proc. IEEE ICC, May 2016, pp. 1–5.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] L. J. Rodriguez, N. H. Tran, T. Q. Duo, T. Le-Ngoc, M. Elkashlan, and S. Shetty, “Physical layer security in wireless cooperative relay networks: State of the art and beyond,” IEEE Commun. Mag., vol. 53, no. 12, pp. 32–39, Dec. 2015.ng

[4] B. Wang, P. Mu, and Z. Li, “Secrecy rate maximization with artificial- noise-aided beamforming for MISO wiretap channels under secrecy outage constraint,” IEEE Commun. Lett., vol. 19, no. 1, pp. 18–21, Jan. 2015.

[5] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, “Outage constrained secrecy throughput maximization for DF relay networks,” IEEE Trans. on Commun., vol. 63, no. 5, pp. 1741–1755, May 2015.

[6] P. Mu, X. Hu, B. Wang, and Z. Li, “Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint,” IEEE Commun. Lett., vol. 19, no. 12, pp. 2174–2177, Dec. 2015.