International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 08, Volume 4 (August 2017) www.ijirae.com
DOI: 10.26562/IJIRAE.2017.AUAE10082

ASYMTOTIC ANALYSIS IN SECURED MESSAGE DELIVERY

S.DIVYASRI,
M.Phil.,Research Scholar/ Computer Science
Sri Jayendra Saraswathy Maha Vidyalaya College of Arts & Science, Coimbatore
[Affiliated to Bharathiar University, Coimbatore]
divyasri19.sekar@gmail.com

PRAVEENTAJ,
Associate Professor/ Computer Science
Sri Jayendra Saraswathy Maha Vidyalaya College of Arts & Science, Coimbatore
[Affiliated to Bharathiar University, Coimbatore]

Manuscript History
Number: **IJIRAE/RS/Vol.04/Issue08/AUAE10082**
DOI: 10.26562/IJIRAE.2017.AUAE10082
Received: 21, July 2017
Final Correction: 31, July 2017
Final Accepted: 08, August 2017
Published: **August 2017**
Citation: **DIVYASRI.S & PRAVEENTAJ (2017). ASYMTOTIC ANALYSIS IN SECURED MESSAGE DELIVERY. International Journal of Innovative Research in Advanced Engineering, Volume IV, 10-14. doi: 10.26562/IJIRAE.2017.AUAE10082**
Editor: Dr.A.Arul L.S, Chief Editor, IJIRAE, AM Publications, India

Abstract: Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. For such a reasons this technology has become popular. Though it is familiar, its wireless channel is vulnerable to the eavesdroppers during message delivery (security is the major problem). In the previous cases this problem was solved by cryptographic methods such as RSA public key cryptosystem. But due to expensive key distribution and improvement in decoding technology, the message transmitted is said to be unsecured. The problem can be overcome by using artificial noise generation. This paper investigates and studies how to deliver the message securely in the wireless network using artificial noise generation concept.

Keywords: Artificial noise generation, Eavesdroppers, Secrecy capacity, Asymptotic, analysis, message, delivery.

I. INTRODUCTION

Although wireless technology is quick and less expensive its channels facilitate two major problems such as network jamming and eavesdroppers attack. The existing systems are based on cryptographic methods which encounters various limitations especially when the network size became vast. In order to overcome such limitations, this paper focuses on artificial noise generation concept where the eavesdroppers are suppressed and confused due to noise transmissions.

More precisely, we assume each receiver is equipped with three ports, one for message receiving and the other two for simultaneous artificial noise generation to suppress eavesdroppers' channel. This differ our noise generation pattern from existing system. Thus the secrecy capacity of the network is also improved.

International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 08, Volume 4 (August 2017) www.ijirae.com
DOI: 10.26562/IJIRAE.2017.AUAE10082

Artificial Noise Generation (ANG) characteristics over the following advantages:

- The ANG guarantee the secret transmission.
- The channel capacity of the receiver is stronger than the eavesdropper.
- The ANG system suppresses the eavesdropper data receiving signal.
- The ANG method generates noise to degrade eavesdroppers' channel. This is known as channel fading.
- This system enhances network security through Inference Cancellation.
- Network jamming is also prevented by this system.

This paper presents a study of benefits of artificial noise generation based on wireless communication to improve the security of messages transmitted through wireless channel which is vulnerable to eavesdropper.

II.ARTIFICIAL NOISE GENERATION

The secure transmission of information in wireless networks without knowledge of eavesdropper channels or locations is considered. Two key mechanisms are employed: artificial noise generation from system nodes other than the transmitter and receiver, and a form of multi-user diversity that allows message reception in the presence of the artificial noise. We determine the maximum number of independently-operating and uniformly distributed eavesdroppers that can be present while the desired secrecy is achieved with high probability in the limit of a large number of system nodes.

While our main motivation is considering eavesdroppers of unknown location, we first consider the case where the path-loss is identical between all pairs of nodes. In this case, a number of eavesdroppers that is exponential in the number of systems nodes can be tolerated. In the case of uniformly distributed eavesdroppers of unknown location, any number of eavesdroppers whose growth is sub-linear in the number of system nodes can be tolerated. The proposed approach significantly outperforms the secured message transmission by the noise transmission.

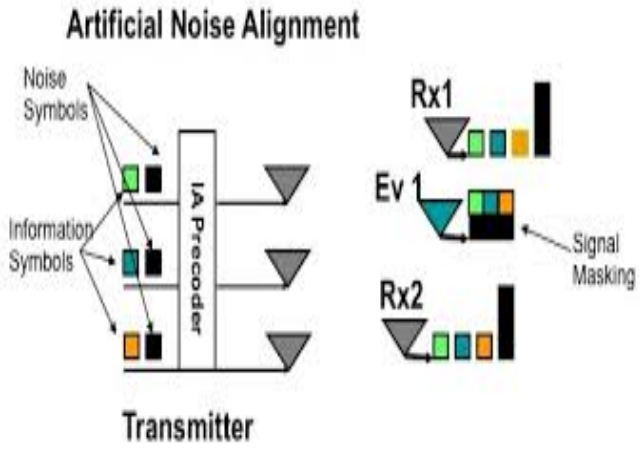

Figure 1: Artificial Noise Alignment

Eavesdroppers:

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. The term *eavesdrop* derives from the practice of actually standing under the eaves of a house, listening to conversations inside. Eavesdropping is the process of gathering information from a network by snooping on transmitted data. And to eavesdrop is to secretly overhear a private conversation over a confidential communication in a not legally authorized way. The information remains intact, but its privacy is compromised.

It can take place over wired networks as over wireless networks. On wired network the operation of eavesdropping is more difficult because it needs the eavesdropper to tap the network, using a network tap which is a hardware device that provides a way to access the data flowing across the network. And that of course can't be achieved unless the eavesdropper can be in touch with the wire of the network which is difficult sometimes and impossible the other times. Eavesdropping can also take place on wireless networks where the eavesdropper is not obliged to be in the dangerous position of being compromised. All what he needs is a computer supplied by a wireless network adapter working on promiscuous mode to allow a network device to intercept and read each network packet that arrives even with other network address, to be in the area of the wireless network coverage and to have one of the particular software tools that allows the eavesdropping.

International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 08, Volume 4 (August 2017) www.ijirae.com
DOI: 10.26562/IJIRAE.2017.AUAE10082

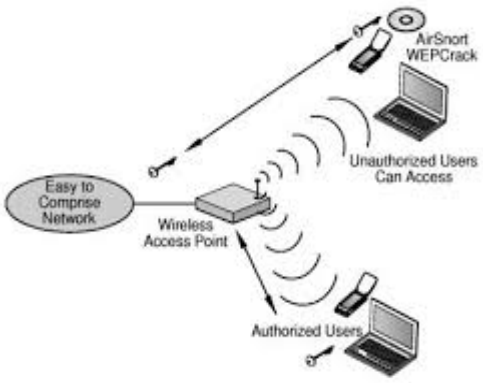

Figure 2: Process of Eavesdropping

Types of Attacks:

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur. There are five types of attack:

1.) Passive attack
2.) Active attack
3.) Distributed attack
4.) Insider attack
5.) Close – in attack

Passive Attack:

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack:

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack:

A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack:

An **insider attack** involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 08, Volume 4 (August 2017) www.ijirae.com
DOI: 10.26562/IJIRAE.2017.AUAE10082

Close-in Attack:

A **close-in attack** involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

One popular form of close in attack is **social engineering** in a social engineering attack; the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

Secrecy capacity:

For the wireless communication systems involving fading channels, their instantaneous secrecy capacity can still be positive even in the case that the eavesdropper channel is stronger than the main channel on the average. This is because legitimate transmitter may exploit the fading fluctuations and send messages to legitimate receiver via opportunistic transmissions. As a fundamental notion in information-theoretic secrecy the secrecy capacity is related to the signal-to-interference-plus-noise ratio (SINR).

For simplicity, we denote uniform transmission power as P_t and uniform noise generation power as P_r. The path loss between node i and node j is denoted by $l(x_i, x_j)$, which can be expressed as $l(x_i, x_j) = min(1, d_{ij}^{-\alpha})$. Here, d_{ij} is the transmission distance and the loss exponent $\alpha > 2$. When node i is transmitting messages to node j, the signal-to-interference-plus-noise ratio (SINR) received by node j over a channel of unit bandwidth can be given by

$$\mathrm{SINR}_{ij} = \frac{P_t l(x_i, x_j)}{N_0 + \sum_{k \in \mathcal{T} \setminus \{i\}} P_t l(x_k, x_j) + \sum_{k \in \mathcal{R} \setminus \{j\}} P_r l(x_k, x_j)}$$

Where,

N_0 denotes ambient noise power at the receiver.
P_t denotes the power to transmit packets.
P_r denotes the power to generate noise.

The SINR received by eaves dropper e can be represented by

$$\mathrm{SINR}_{ie} = \frac{P_t l(x_i, x_e)}{N_0 + \sum_{k \in \mathcal{T} \setminus \{i\}} P_t l(x_k, x_e) + \sum_{k \in \mathcal{R}} P_r l(x_k, x_e)}.$$

Therefore we make the following assumptions in order to demonstrate the Usefulness of the artificial noise generation. In our model, both channel state information (CSI) and the position information of eaves droppers are assumed to be unknown to legitimate nodes. It can be seen from the following figure.

That there exists a gap between the lower bound and the upper bound of per-node capacity, when the intensity of eavesdroppers is in the range $[\theta(n^{-\beta}), \theta(\log^{\alpha-2/\alpha} n)]$.Thus, it turns out to be a tempting issue whether the secrecy capacity can be improved if some of the information is known. Note that the gap is caused by the randomness in Poison distribution since a jump of log n number of nodes per unit area occurs at the point $\psi_e = 1$. Where ψ_e is the expected density of eaves dropper.

Taking the concurrent transmission range for instance, it has to be set uniform over the whole network to guarantee the transmission secrecy for each T-R pair in the worst case. However, it can be solved in the case where the information such as the positions of eavesdroppers is known. Different artificial noise generation powers and different concurrent transmission ranges can be exhibited at different T-R pairs.

International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 08, Volume 4 (August 2017) www.ijirae.com
DOI: 10.26562/IJIRAE.2017.AUAE10082

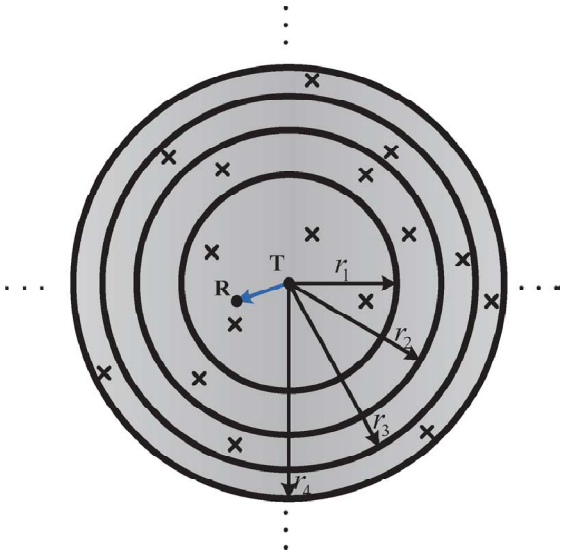

Figure 3: Illustration of Network Partition

Hence, it is possible to narrow this gap by appropriate adjustments on the number of concurrent transmission nodes as well as the corresponding TDMA schemes, which results into capacity improvement.

III.CONCLUSION

Secrecy of message delivery is a major concern in a lot of real applications. In the previous work, the asymptotic behavior of secrecy capacity in an ad hoc network (where both the channel state information and locations of eavesdroppers are unknown) was studied. This proposed paper analyzes the security technique using the artificial noise generation system suitable for secrecy of message delivery in large scale wireless networks. Here the secrecy issue in large-scale networks are strongly correlated with the node distributions of both legitimate nodes and eavesdroppers, also depends on how the packets is delivered across the network. Hence, the relationship between the secrecy capacity and the heterogeneity Distributions of nodes is also studied.

REFERENCES

1. S. Goel and R. Negi, for guaranteeing secrecy using artificial noise, (2008).
2. T. Liu and S. Shamai, for Secrecy capacity of the multiple antenna wiretap channel, (2009).
3. A. Khist and G. W. Wornell, for Secure transmission with multiple antennas, (2010).
4. O.Koyluoglu, E. Koksal, and E. Gammel, for on secrecy capacity scaling in wireless networks, (2012).
5. Jinbei Zhang, Luoyi Fu, and Xinbing Wang, for Asymptotic Analysis on Secrecy Capacity in Large-Scale Wireless Networks,(2014).

