ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

A Survey: Proactive Eavesdropping Via Jamming To Defend Against Suspicious Communication Link

Raaga Darshini G[1] , Dr Sampoornam K P[2]

PG Student, Dept of ECE, Bannari Amman Institute of Technology, Erode Tamil Nadu, India[1]

Associate Professor, Dept of ECE, Student, Bannari Amman Institute of Technology, Erode Tamil Nadu, India[2]

ABSTRACT: Wireless security assumes that the wireless communication is legitimate and goals to protect them against these attacks. The emerging infrastructure less wireless communication can be illegally used by terrorists and are very difficult to monitor and becomes threat to public security. To avoid these, legitimate eavesdropping and jamming attacks used jointly to prevent against wireless attacks. Here the eavesdropping is used to intercept and decode the sufficient information from the suspicious source for deciding future measures against them and jamming is used to disable or disrupt the suspicious destination. This paper proposes the survey of legitimate eavesdropping and jamming attacks. The eavesdropping and jamming attacks are adopted by both legitimate users and suspicious users for their intention tasks. Numerical results shows that the average eavesdropping rate and the jamming power of the legitimate monitor.

KEYWORDS: Eavesdropping, Jamming, Legitimate monitor.

I. INTRODUCTION

Wireless security has become more attracted topic among lot of researchers recently, and there are works investigating about defense mechanisms to secure the wireless communication against wireless attacks. Security is the most important component to most of the wireless networks since, hackers were discovered number of wireless attacks to steal and spoof the content of the information from the legitimate wireless communication. The wireless attacks were Black hole attack, Worm hole attack, Black hole attack, Denial of service attack, Sybil attack, Selective forwarding attack, Eavesdropping and Jamming. Wireless networks consists of number of sensors that have limited resources like low bandwidth, limited battery supply and low memory and they are tiny in size and are intended to perform their tasks efficiently. These sensors were used in real time applications like patient monitoring in hospitals, military and forest monitoring. So secured data transmission without any data loss is essential. For such applications, wireless information's should be highly confidential. But, due to the vulnerable nature the sensor networks, adversary users may steal or leak the wireless information by deploying malicious nodes into the wireless network. There is a developing need for authorized users such as government agencies to implement the new wireless surveillance methods to monitor the adhoc wireless suspicious communication legitimately[10-13].

In this paper, defense mechanism against wormhole attack is employed by introducing legitimate eavesdropping and jamming. Eavesdropping may overhear the wireless information if it is within the range of the transmitting node and in jamming, legitimate monitor send jamming signals to the suspicious receiver to reduce the signal reception.

II. LITERATURE SURVEY

Proactive Eavesdropping via Jamming for Rate Maximization Over Rayleigh Fading Channels [1], here the authors proposed a method in wireless security from preventing new legitimate surveillance from the conventional

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

eavesdropping attacks. They consider a setup shown in Fig. 1, a legitimate monitor goals to eavesdrop a wireless communication link over Rayleigh fading channels. Here the suspicious transmitter controls its communication rate to maintain receiver the proper target outage probability. By this, the legitimate monitor can successfully decode the data and eavesdrop the suspicious communication link when its data rate is larger than the suspicious communication rate. If the monitor is far away from the suspicious transmitter, then wireless channels may fluctuate significantly over time. To overcome this issue, they proposed a method called proactive eavesdropping via jamming, legitimate monitor which operates in full duplex mode and to moderate the communication rate of the suspicious transmitter, it sends the jamming signals for the simultaneous eavesdropping.

In Fig 1, they consider a legitimate surveillance scenario, a legitimate monitor in full duplex mode goals to eavesdrop a suspicious communication link via jamming. Here the legitimate monitor is implemented with two antennas, one for eavesdropping(transmitter) and another one for jamming(receiver) and the suspicious transmitter and receiver, each implemented with one antenna. In any time block, let L1 denotes the power gain from suspicious transmitter to the receiver, L2 denotes the power gain from the suspicious transmitter to the legitimate monitor's eavesdropping antenna and L3 denotes the power gain of the legitimate monitor's jamming antenna to the suspicious receiver. They assumed that the legitimate monitor don't know the Channel State Information(CSI) of L0 and L2 at every time block, but it knows their Channel Distribution Information(CDI) and the channel L1 is known at the legitimate monitor in each time block.

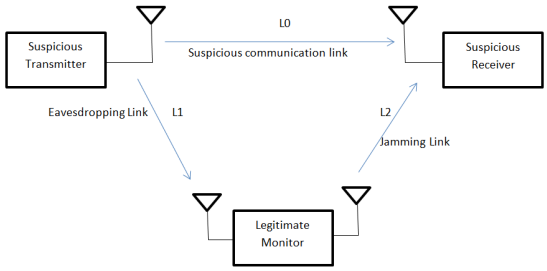

Fig.1. A wireless legitimate surveillance Scenario

They considered that the suspicious transmitter transmits signal with a constant power P, at the same time as the legitimate monitor sends a jamming power Q to interfere with the suspicious receiver for the simultaneous eavesdropping. The self interference in the legitimate monitor from the eavesdropping antenna to the jamming antenna is cancelled by using analog to digital self interference cancellation methods. The suspicious transmitter adjusts its communication rate to maintain proper outage probability and to less the data rate of the suspicious link, the monitor adjust the jamming power and thus reducing the suspicious communication rate. A larger jamming power can reduce the fixed transmission rate more significantly, which helps in improving the non outage probability at the legitimate probability. Fig.5(a) and 5(b), shows the numerical results of the average eavesdropping rate of the legitimate monitor.

Pilot Contamination for Active Eavesdropping [2], authors discussed about how an active eavesdropper can attack the training phase in wireless communication. They derived a new security attack based on pilot contamination phenomenon, which targets at systems using reverse training to obtain the channel state information at the transmitter for precoder design. This attack changes the legitimate transmitter precoder to strengthen the received signal during data transmission at the eavesdropper.

The pilot contamination attacks the transmitter which designs its precoder itself based on the estimation of the legitimate communication link's CSI and it is done by the receiver sends its pilot signals to facilitate the channel estimation at the transmitter, i.e. reverse training. During reverse training, the eavesdropper also sends the pilot signals to spoof the transmitter for the estimation of the correct channel. Thus the transmitter incorrectly designs its precoder which results in signal reception in the eavesdropper during data transmission. The eavesdropper transmits signal in random jamming noise to reduce the signal reception at the legitimate receiver, the pilot contamination attack transmits signals with the goal of improving the signal reception at the eavesdropper.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

From the Fig. 2, they considered the data transmissions from the legitimate transmitter, Alice, to the receiver Bob, and in the presence of an eavesdropper, Eve. Alice is implemented with more than one antennas, Bob and Eve implemented with single antenna either for transmission or reception. The channel from Alice to bob and eve, Bob to Alice and eve to Alive and Bob had both path loss attenuation and fading gain. The fading gain of Alice to Bob is equal due to channel reciprocity and the path loss attenuation of Alice to Bob is not necessarily equal to Bob to Alice.

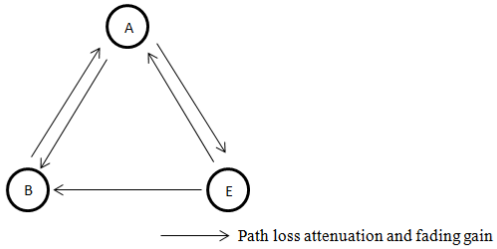

Fig.2. Wireless communication channel between Alice(A), Bob(B) and Eve(E).

Here, they described the pilot contamination attack, when the reverse training phase is done by Alice and Bob and is also known by Eve. The training phase can be easily obtained by Eve because it is fixed and repeatedly used used over time. This makes an opportunity for an eavesdropper to make an impact on the channel estimation of the Alice. Eve transmits pilot signal to Alice at the same time as Bob transmits during the reverse training phase. This makes Alice estimation of her outgoing channel to Bob as well as Eve. The advantages to Bob in pilot contamination attack are: it degrades the Alice estimation accuracy of outgoing channel to Bob and more necessarily by attacking the beam forming design of Alice, it helps in data detection at Eve.

Wireless Information Surveillance via Proactive Eavesdropping with Spoofing Relay [3], here they discussed about the new proactive eavesdropping via spoofing relay, the legitimate monitor operates in full duplex mode with simultaneous eavesdropping and spoofing relay to change the transmission rate of the source for better eavesdropping performance. In legitimate monitor, the received signal at each antenna is divided into two parts, one for information eavesdropping and other for spoofing relay.

Passive eavesdropping is the proper approach for wireless information surveillance, where the legitimate monitor only listens the suspicious wireless channel to decode their information and this approach will be effective only when the channel from suspicious transmitter source to the legitimate monitor is better than the channel from suspicious source to destination. But in practice, this does not happen when the legitimate monitor is far away from the suspicious transmitter compared to suspicious receiver. For the given power budget for jamming, the eavesdropping performance cannot be improved if the eavesdropping channel capacity is less than the suspicious channel and also there are other scenarios to achieve higher eavesdropping rate, the legitimate monitor can spoof the suspicious transmitter to increase its transmission rate.

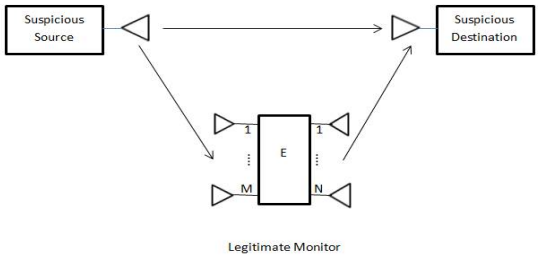

Fig.3. Wireless information surveillance via legitimate multi antenna monitor.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

To enhance the surveillance capability of legitimate monitor, instead of eavesdropping the information, the legitimate monitor also send some spoofing signals to the suspicious receiver and change the transmission rate of the transmitter for better eavesdropping performance. The legitimate monitor will improve the suspicious channel by sending source signal to the suspicious receiver if the suspicious link if no better than the eavesdropping link which leads higher transmission rate by suspicious transmitter and higher eavesdropping rate. If the suspicious link is stronger than the eavesdropping link, the legitimate monitor will reduce the suspicious link channel by sending jamming signals to the suspicious receiver to spoof the suspicious transmitter so as to degrade its transmission rate.

Proactive Eavesdropping via Cognitive Jamming in Fading Channels[4], here the aim of the legitimate monitor is to intercept the suspicious communication link and it can successively decode (eavesdrop) the information only when the data rate at the eavesdropping antenna is greater than the suspicious receiver. In this letter, the legitimate monitor intended to jam the receiver to reduce the data rate so as to decode efficiently.

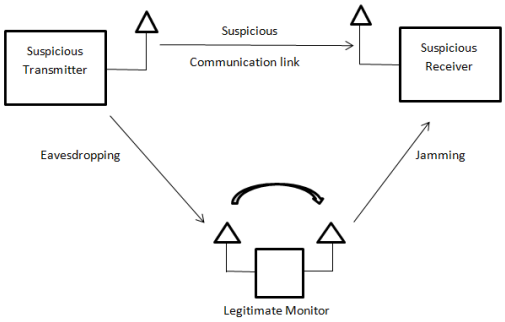

Fig.4(a). Co located eavesdropping antenna and jamming antenna.

From the Fig.4(a), the legitimate monitor goals to intercept the wireless link from the suspicious transmitter to the suspicious receiver over fading channels, so that the legitimate monitor can decode the information successfully from the communication link only when the SNR of the legitimate monitor is greater than the suspicious receiver. By this the legitimate monitor can be able to eavesdrop the entire information as same as the suspicious receiver. In practice, if the legitimate monitor is located far away from the suspicious transmitter, it cannot be able to eavesdrop properly. To overcome this , they proposed the new work to improve the performance of the legitimate eavesdropping.

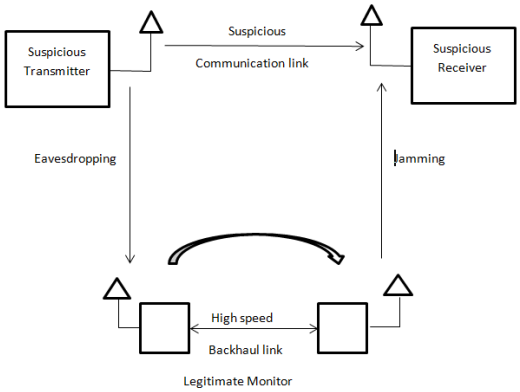

Fig.4(b). Separate eavesdropping antenna and jamming antenna.

The authors proposed this approach in Fig where the full duplex legitimate monitor intended to send jamming signals to the suspicious wireless link, to reduce the data rate of the suspicious receiver for eavesdropping the suspicious

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

transmitter efficiently. The eavesdropping antenna and jamming antenna can be either co located or separately located Fig 1-(a) and (b), for such full duplex legitimate monitor. For co located design of eavesdropping and jamming facilitate the joint operation, but may be lead to heavy self interference from the eavesdropping antenna to the jamming antenna. This self interference can be perfectly cancelled by practical analog to digital converter(ADC). For separate structure, to enable the joint operation it requires the low latency backhaul link to connect the both antennas. For both co located and separate approaches, to increase the jamming for decoding, for the limited jamming power constraint according to various fading state, it is necessary for the legitimate monitor to control the jamming power.

III. PROPOSED METHOD

Wireless Security has become more important component to current wireless networks and attackers have deployed malicious nodes into the network to leak or spoof the content of the information from the legitimate users. One of the ways to overcome this, to disable the communication between suspicious users.

To degrade or disable the malicious communication link, SID uses its all transmission power to send artificially generated Gaussian signal. If the data rate is reduced below the B's QOS requirements, A will stop transmission. Suspectably, the noise jamming is detected by both A and B by measuring the noise level. So we propose that SID jams the B by combining the processed version of eavesdropped signal from A and Gaussian noise. If such signal is sufficiently strong and combined destructively at B with the direct signal from A, the direct signal will be perfectly cancelled without the noise level increased. If the suspicious communication employs HARQ protocol, SID can spoof the ACK from B to A to NACK, so A will stop transmission.

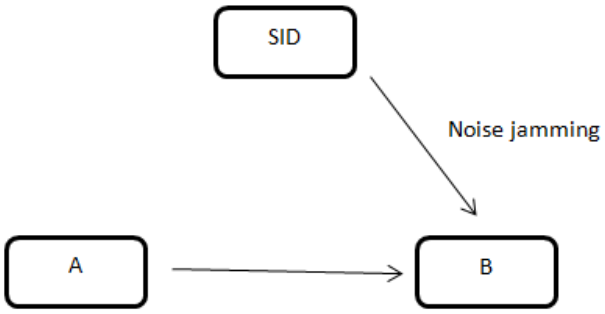

Fig.3.1. SID jams by sending combining eavesdropped signal and Gaussian signal.

IV. EXPERIMENTAL RESULTS

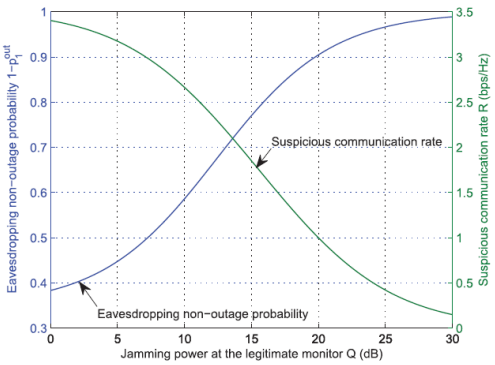

Fig.5(a). The non outage probability of eavesdropping and suspicious communication rate versus jamming power of the legitimate monitor.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

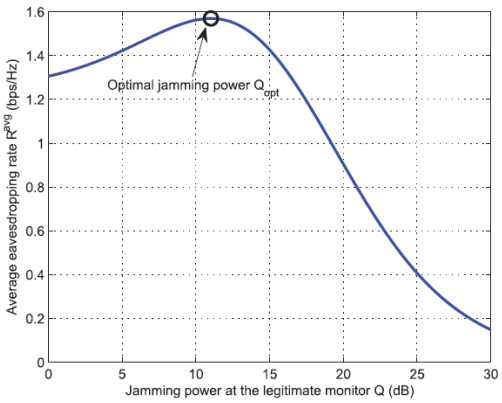

Fig.5(b). The eavesdropping rate versus jamming power of the legitimate monitor.

V. CONCLUSION

This paper proposes the survey of joint legitimate eavesdropping and jamming method against suspicious wireless communication, where legitimate monitor will eavesdrop the source of the suspicious communication and jams the receiver by sending jamming signals to improve the performance of eavesdropping and to degrade the signal reception at suspicious receiver. In [2], the authors assumed that there is no self interference between eavesdropping and jamming antenna. In practice, that is not possible and there will be some self interference between eavesdropping and jamming antenna.

REFERENCES

[1] J. Xu, L.Duan and R.Zhang,"Proactive eavesdropping via jamming for Rate Maximization over Rayleigh Fading channels,"IEEE Wireless Communications. Letters, vol. 5,no. 1, Feb.2016, pp.80-83.
[2] X.Zhou, B.Maham and A.Hjorugnes, "Pilot Contamination for Active Eavesdropping, "IEEE Trans. Wireless Communications, vol. 11, no.3, Mar. 2012, pp. 903-07.
[3] Y. Zeng and R.Zang,"Wireless Information Surveillance via Proactive Eavesdropping with Spoofing Relay, "IEEEJ.Sel. Topics Signal Process., vol.10, no.8, Dec.2016, pp. 1449-61.
[4] J.Xu, L. Duan and R.Zhang,"Proactive Eavesdropping via Cognitive Jamming in Fading channels," Proc. IEEE ICC, 2016, pp. 1-6.
[5] Terrorist Surveillance Program [online] Available: https://en.wikipedia.org/wiki/Terrorist_Surveillance_Program.
[6] G.T.Amariucai and S.Wei,"Half duplex active eavesdropping in fast fading channels: A block-Markov Wyner secrecy encoding scheme, "IEEE Trans. Inf.Theory,vol.58,no.7,pp.4660-4677,jul. 2012.
[7] A.Mukherjee and A.L.Swindlehurst. "Jamming games in the MIMO wiretap channel with an active eavesdropper."IEEETrans.Inf.Theory.
[8] "A Full dulplex active eavesdropper in MIMO wireless channels: construction and counter measures," in Proc.2011 Asilomar Conf. on Signals, Systems, and Computer.
[9] J.Jose, A.Ashikmin, T.L.Marzetta and S.Vishwaath,"Pilot Contamination and precoding in multi-cell TDD systems," IEEE Trans. Wireless Communications. vol.10, no.8, pp. 2640-2651,Aug.2011.
[10] T.L.Marzetta."How much training is required for multiuser MIMO?" in Proc.2006 Asilomar Conference on signals, systems and Computers,pp. 359-363.
[11] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, [Online]. Available: https://arxiv.org/abs/1612.07859
[12] J. Xu, L. Duan, and R. Zhang, "Fundamental rate limits of physical layer spoofing," *IEEE Wireless Commun. Lett.*, to be published.
[13] J. Xu, L. Duan, and R. Zhang, "Transmit optimization for symbol-level spoofing with BPSK signaling," in *Proc. IEEE GLOBECOM Workshop*, Dec. 2016, pp. 1–6.