ISSN 2395-1621

A Survey on Protection of Data Aggregation against Identity Deception Attacks

[#1]Jyoti Rajgade, [#2]Prof. Santhosh Waghmode

[1]jsrajgade@gmail.com
[2]stwaghmode@gmail.com

[#12]Department of Computer Engineering

Imperial College of Engineering and Research,
Wagholi, Pune.

ABSTRACT

In this paper we Survey on wireless networking using the different network attack technique. Considering the role of wireless adversary, which targets the packets of high importance by emitting radio frequency signals and do not follow underlying network architecture. Typically, jamming attacks have been considered under external threat model, in which jammer is not part of network. We examine identity deception attacks in WSN, used by criminals to steal personal information and I will discuss countermeasures that can be used to defend against these attacks. In this paper we proposed the new attack on WSN, carousel attack and stretch attack during the packet forwarding source to destination.

Keywords: WSN, Security, Routing, Ad hoc networks, Carousel attack, Stretch attack.

ARTICLE INFO

Article History

Received: 5th June 2017

Received in revised form :

5th June 2017

Accepted: 10th June 2017

Published online :

17th June 2017

I. INTRODUCTION

Wireless networks have paved the way for mobile nodes to communicate with each other. The two basic system models are fixed backbone wireless system and wireless Mobile Ad hoc Network (MANET).[2][3] A MANET is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. Therefore the functioning of ad hoc networks is dependent on the co-operation of each and every node. The nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. The rapid proliferation of wireless ad-hoc networks and mobile computing applications has changed the landscape of network security. Wireless networks are networks which provide users with connectivity regardless of their actual physical location. WSN's (Wireless sensor Networks) are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. [6]

Jamming Attack: - Jamming attack comes under the category of DOS. There are various ways or we can say strategies which can be performed by jammer with the help of which jammer can interfere with other wireless communications. Here are some of the strategies explained that can be performed:-

Constant Jammer: Here there is continuous emission of radio signals occurs. This represents the radio bits. Here any MAC protocol is not followed to generate signal.

Deceptive Jammer: Instead of random bit, it continuously emits regular packets. . It deceive other nodes to believe that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies. As compared to constant jammer it is difficult to recognize constant jammer.

Random Jammer: It intermittently transmits both random bits and regular packets. It continuously switch between the two

phases :sleep phase and jamming phase. There is not any particular time for sleep phase and jamming phase. We can adjust tradeoff between efficiency and effectiveness by adjusting the ratio of these two times.

Reactive Jammer: When reactive jammer senses that somebody is not there it doesn't waste its resources in only jamming. Here the target of reactive jammer is that sender as well as receiver tries to input the noise by modifying the bits as many as possible. But this modification should occur at a low power. Due this low power it is able to identify that bit and so that it can be removed at receiver when checksum is performed over that bit.

II. OBJECTIVES OF NETWORK DESIGN

Small node size: The sensor nodes are generally deployed in a harsh and hostile environment, So if we reduce the node size it will facilitate the node deployment. The advantages of small node size is it will require low power as well as low cost.

Low node cost: As previously explained because the environment used for sensor deployment reducing the size of sensors will result in reducing cost also.

Low power consumption: Here the problem is that sensor nodes are battery powered, hence if the battery is discharged it will require human interference or else it will negatively impact on the system, hence it is a very crucial task to maintain the battery power.

Scalability: Here the nodes in a sensor are arranged in the order range of tens ,hundreds or thousands. Hence to maintain different network sizes ,the network protocol for sensor design should be scalable .

Reliability To ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels, network protocols designed for sensor networks must provide error control and correction mechanisms

Self-configurability: In the sensor network the nodes should have ability to configure themselves according to the connectivity or in case of failure once they are deployed.

Adaptability: The network protocols should be flexible and adaptive to network density because the network density may get changed since in a network the number of nodes may get changed due to failure or they get moved.

Security: Here it's obvious that sensors contains some sensitive information so that there should be a security to prevent from unauthorized access over the data.

III. REVIEW OF LITERATURE

Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", in this paper studied a CPS scenario where a malicious agent carries out jamming attacks on the communication channel between a sensor and a remote estimator. he first considered a situation where the sensor and the attacker fix their strategies apriori. For the case where the sensor and the attacker have on-line information about the previous transmission outcomes and the occurrence of attacks. [1]

Zhuo Lu,Student, "Modeling, Evaluation and Detection of Jamming Attack in Time-Critical Wireless Applications", in this paper, he provided an in-depth study on the impact of jamming attacks against time-critical smart grid applications by theoretical modelling and system experiments. He introduced a metric, message invalidation ratio, to quantify the impact of jamming attacks. He showed via both analytical analysis and real-time experiments that there exist phase transition phenomena in time-critical applications under a variety of jamming attacks. Based on our analysis and experiments, He designed the JADE system to achieve efficient and robust jamming detection for power networks. [2]

Nani Yalu, RajatSubhra Goswami, Subhasish Banerjee, "An Efficient Packet Hiding Method for Preventing Jamming Attacks in Wireless Networks", this paper have reviewed all packet hiding methods and addressed their merits and demerits. We have also compared different packet hiding methods and thus come up with the conclusion that all three packet hiding methods are highly secured but have their own shortfalls.[3]

Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems,", in this paper, author characterize of the reachable set of the system state and estimation error under the attack, which provides a quantitative measure of the resilience of the system. In this system at end, he will explain an ellipsoidal algorithm to compute the outer approximation of the reachable set. He also prove a necessary condition under which the reachable set is unbounded, indicating that the attacker can successfully destabilize the system. [4]

Saurabh Amin, Alvaro A. C´ardenas, and S. Shankar Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks" in this paper he considers the network security problem constrained optimal control for discrete-time, linear dynamical systems in which control and measurement packets are transmitted over a communication network. The packets may be jammed or compromised by a malicious adversary. For a class of denial-of-service (DoS) attack models, the goal is to find an (optimal) causal feedback controller that minimizes a given objective function subject to safety and power constraints. He present a sem definite programming based solution for solving this problem. [5]

Yi-Kuo Yu, Yi-Cheng Zhang, Paolo Laureti, Lionel Moret, "Decoding Information from noisy, redundant, and intentionally-distorted sources", here author establish a framework to systematically tackle the challenging problem of information decoding in the presence of massive and redundant data. When applied to a voting system, our method simultaneously ranks the raters and the ratees using only the evaluation data, consisting of an array of scores each of which represents the rating of a ratee by a rater. [6]

Rong-Hua Li, Jeffery Xu Yu, Xin Huang, Hong Cheng, "Robust Reputation-Based Ranking on Bipartite Rating Networks" this paper propose six new reputation-based algorithms, where the users' reputation is determined by the aggregated difference between the users' ratings and the corresponding objects' rankings. We prove that all of our algorithms converge into a unique fixed point. The time and space complexity of our algorithms are linear w.r.t. the size of the graph, thus they can be scalable to large datasets. [7]

IV. CONCLUSION

n this paper, we review the attacks in wireless networks. We also analysis system models to introduce carousel attack and stretch attack during the packet forwarding source to destination. We also attack detection model is also presented in proposed system. Then we discussed real-time packet classification to classify the packet before reaching at destination.

ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. S.T.Waghmode Sir for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 60, NO. 10, OCTOBER,2015.

[2] Zhuo Lu,Student Member, IEEE,Wenye Wang,Senior Member, IEEE, and Cliff Wang,Senior Member, IEEE "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 8, AUGUST 2014.

[3] Nani Yalu, RajatSubhra Goswami, Subhasish Banerjee, "An Efficient Packet

Hiding Method for Preventing Jamming Attacks in Wireless Networks" IEEE WiSPNET 2016.

[4] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in Proc. 1st Int. Conf. High Confidence Networked Syst., 2012, pp. 47–54.

[5] Saurabh Amin, Alvaro A. C´ardenas, and S. Shankar Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks" R. Majumdar and P. Tabuada (Eds.): HSCC 2009, LNCS 5469, pp. 31–45, 2009. c Springer-Verlag Berlin Heidelberg 2009.

[6] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A Statistical Mechanics and its Applications, vol. 371, pp. 732–744, Nov. 2006.

[7] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation-based ranking on bipartite rating networks," in SDM'12, 2012, pp. 612–623.

[8] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," in Proceedings of the 2009 IEEE international conference on Symposium on Information Theory -Volume 3, ser. ISIT'09, 2009, pp. 2051–2055.

[9] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," ArXiv e-prints, Aug. 2012.

[10] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a comment rating environment," in Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, ser. KDD '11, 2011, pp. 159–167.

[11] C. T. Chou, A. Ignatovic, and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 8, pp. 1525–1534, Aug 2013.

[12] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wire-less sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867 – 880, 2012, ¡ce:title¿Special Issue on Trusted Computing and Communications¡/ce:title¿.

[13] H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A game-theoretic approach for high-assurance of data trustwor-thiness in sensor networks," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on, april 2012, pp. 1192 –1203.

