ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

A Survey on Security Optimization of Dynamic Networks with Graph Modelling

Dr. P.Senthilvadivu[1], S.Vishnupriya[2]

Associate Professor & Head, Department of BCA Hindusthan College of Arts and Science, Coimbatore, India[1]

M.Phil Research Scholar – Computer Science, Hindusthan College of Arts and Science, Coimbatore, India[2]

ABSTRACT: Wireless network technology is most frequently used network technology. A number of variants are available on the basis of traditional wireless networking such as MANET and others. This paper is to review of various secure routing protocols and Quality of Service (Qos) methods. Meanwhile, this paper illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by explaining the main specifications of the common security standards like 802.11 protocol. Moreover, it explains the concept of secure routing protocol in graph modeling and its security specifications. Finally, it sums up with thoughts and suggestions about wireless security, along with a chosen example of the current proposals in wireless security.

KEYWORDS: Secure routing; Manets; Graph; QoS; Attacks

I. Introduction

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. Over the past few years, the wireless network has almost exploded due to the rapid development of the Internet, and also the growth of small mobile devices as an instrument of communication and data exchange. The most used today is a wireless network built on top of a wired network. The wireless nodes are able to act as bridges in a wired network called base-stations. An example of this wireless network is the cellular phone networks where a phone connects to the base-station with the best signal quality. The movement of the mobile devices is facilitated by moving communication cells from one base-station to another base-station. The main infrastructure requires a complex administrative work.

Large organizations need rigorous security tools for analysing potential vulnerabilities in their networks. However, managing large-scale networks with complex configurations is technically challenging. For example, organizational networks are usually dynamic with frequent configuration changes. These changes may include changes in the availability and connectivity of hosts and other devices, and services added to or removed from the network.

Network administrators also need to respond to newly discovered vulnerabilities by applying patches and modifications to the network configuration and security policies, or utilizing defensive security resources to minimize the risk from external attacks. For instance, to prevent a remote attack targeting a host it is useful to analyze the candidate defensive strategies in choosing installation and runtime parameters for one or several intrusion prevention system. To facilitate a scalable security analysis of organizational networks, attack graphs (e.g., [1], [2]) were proposed. Attack graphs show possible attack paths with respect to a particular network setting, which provide the necessary elements for modeling and improving the security of the network.

Large organizations need rigorous security tools for analyzing potential vulnerabilities in their networks. However, managing large-scale networks with complex configurations is technically challenging. For example, organizational networks are usually dynamic with frequent configuration changes. These changes may include changes in the availability and connectivity of hosts and other devices, and services added to or removed from the network.

DOI: 10.15680/IJIRCCE.2016. 0410049

II. Literature Review

L.H.G. Ferraz, P.B. Velloso, and O.C.M.B. Duarte [3] proposed a robust and distributed access control mechanism based on a trust model to secure the network and stimulate cooperation by excluding misbehaving nodes from the network. The mechanism divides the access control responsibility into two contexts: local and global. The local context responsibility is the neighborhood watch to notify the global context about suspicious behavior. In its turn, the global context analyzes the received information and decides whether it punishes the suspicious node using a voting scheme. To model the exclusion mechanism and perform a parameter analysis. Simulation results prove that the combination of voting and trust schemes provides an accurate and precise classification and node exclusion mechanism, even though in scenarios of limited monitoring.

S. R. Biradar, et al[4] discussed new routing algorithm is quite suitable for a dynamic self starting network, as required by users wishing to utilize adhoc networks. AODV provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements. Nevertheless we can still maintain most of the advantages of basic distance vector routing mechanisms. To show that our algorithm scales to large populations of mobile nodes wishing to form adhoc networks.

J. Mo, M. Tao, Y. Liu, and R. Wang [5] discussed the optimal relay beam former structures. Then, iterative algorithms are proposed to find source and relay beam formers jointly based on alternating optimization. Furthermore, they conduct asymptotic analysis on the maximum secrecy sum-rate. They showed that when all transmit powers approach infinity, the two-phase two-way relay scheme achieves the maximum secrecy sum rate if the source beam formers are designed such that the received signals at the relay align in the same direction. This reveals an important advantage of signal alignment technique in against eavesdropping. It is also shown that if the source powers approach zero, the three-phase scheme performs the best while the two-phase scheme is even worse than direct transmission. Simulation results have verified the efficiency of the proposed secure beam forming algorithms as well as the analytical findings.

Y. Zou, X. Wang, and W. Shen [6] explored the physical-layer security in cooperative wireless networks with multiple relays where both amplify-and-forward (AF) and decode-and-forward (DF) protocols are considered. To propose the AF and DF based optimal relay selection (i.e., AFbORS and DFbORS) schemes to improve the wireless security against eavesdropping attack. For the purpose of comparison, we examine the traditional AFbORS and DFbORS schemes, denoted by T-AFbORS and TDFbORS, respectively.

D. Goeckel, et.al [7] discussed 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. To 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 the main motivation is considering eavesdroppers of unknown location, first is to 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.

A. Sheikholeslami et al, [8] proposed the effectiveness and straightforward implementation of physical layer jammers make them an essential security threat for wireless networks. The authors discussed the reliable communication in a wireless multi-hop network in the presence of multiple malicious jammers is considered. Since energy consumption is an important issue in wireless ad hoc networks, minimum energy routing with and without security constraints has received significant attention in the literature; however, energy-aware routing in the presence of active adversary (jammers) has not been considered. To proposed an efficient algorithm for minimum energy routing between a source and a destination in the presence of both static and dynamic malicious jammers such that an end-to-end probability of outage is guaranteed.

Z. Ding, K. Leung, D. Goeckel, and D. Towsley [9] discussed the information theoretic security has recently emerged as an effective physical layer approach to provide secure communications. The outage performance of such a secrecy communication system is considered in this paper, since it is an important criterion to measure whether users' predefined quality of service can be met. Provided that the legitimate receiver and eavesdropper have the same noise power, many existing secure schemes cannot achieve outage probability approaching zero, regardless of how large the transmission power is. Authors introduced the cooperative transmission into secrecy communication systems, it will be shown here that outage probability approaching zero can be achieved. In particular, scenarios with single-antenna nodes and multiple-antenna nodes will both be addressed, and the optimal design of beam forming/precoding will be investigated. Explicit expressions of the achievable outage probability and diversity-multiplexing tradeoff will be developed to demonstrate the performance of the proposed cooperative secure transmission schemes, and numerical results are presented.

X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes [10] studied the throughput of large-scale decentralized wireless networks with physical layer security constraints. In particular, we are interested in the question of how much throughput needs to be sacrificed for achieving a certain level of security. To considered random networks where the legitimate nodes and the eavesdroppers are distributed according to independent two-dimensional Poisson point processes. The transmission capacity framework is used to characterize the area spectral efficiency of secure transmissions with constraints on both the quality of service (QoS) and the level of security. This framework illustrates the dependence of the network throughput on key system parameters, such as the densities of legitimate nodes and eavesdroppers, as well as the QoS and security constraints. One important finding is that the throughput cost of achieving a moderate level of security is quite low, while throughput must be significantly sacrificed to realize a highly secure network. We also study the use of a secrecy guard zone, which is shown to give a significant improvement on the throughput of networks with high security requirements.

M. Saad [11] suggested a multi-hop wireless network and a source destination pair of nodes to addressed the problem of jointly selecting a communication route and allocating transmit power levels, so that the end-to-end spectral efficiency of the route exceeds a desired threshold. The transmit power level, however, has been assumed to be known, and route selection was considered in isolation. The author presented the first rigorously proven optimal, polynomial-time algorithms for two versions of the joint spectral-efficient routing and power allocation problem: sum-power minimization and maximum power minimization. The algorithm rely on the divide-and conquer principle and the Bellman-Ford algorithm for shortest (or widest) path computation.

C. Wang, H.-M.Wang, and X.-G. Xia [12] studied the cooperative transmission for securing a decode-and-forward (DF) two-hop network where multiple cooperative nodes coexist with a potential eavesdropper. Under the more practical assumption that only the channel distribution information (CDI) of the eavesdropper is known, they proposed an opportunistic relaying with artificial jamming secrecy scheme, where a "best" cooperative node is chosen among a collection of N possible candidates to forward the confidential signal and the others send jamming signals to confuse the eavesdroppers. To first investigate the ergodic secrecy rate (ESR) maximization problem by optimizing the power allocation between the confidential signal and jamming signals. In particular, to exploit the limiting distribution technique of extreme order statistics to build an asymptotic closed-form expression of the achievable ESR and the power allocation is optimized to maximize the ESR lower bound. Although the optimization problems are non-convex, to proposed a sequential parametric convex approximation (SPCA) algorithm to locate the Karush-Kuhn-Tucker (KKT) solutions.

J. Li, A. Petropulu, and S. Weber [13] considered a cooperative wireless network in the presence of one or more eavesdroppers, and exploit node cooperation for achieving physical (PHY) layer based security. Two different cooperation schemes are considered. In the first scheme, cooperating nodes retransmit a weighted version of the source signal in a decode-and-forward (DF) fashion. In the second scheme, referred to as cooperative jamming (CJ), while the source is transmitting, cooperating nodes transmit weighted noise to confound the eavesdropper. They investigated two objectives: i) maximization of the achievable secrecy rate subject to a total power constraint and ii) minimization of the total power transmit power under a secrecy rate constraint. For the first design objective, to obtain the exact solution for the DF scheme for the case of a single or multiple eavasdroppers, while for the CJ scheme with a single eavesdropper we reduce the multivariate problem to a problem of one variable. For the second design objective, existing work introduces additional constraints in order to reduce the degree of difficulty, thus resulting in suboptimal solutions. In this work raised those constraints, and obtains either an analytical solution for the DF scheme with a single eavesdropper, or reduces the multivariate problem to a problem of one variable for the CJ scheme with a single eavesdropper.

C. Ma, et al. [14] discussed a Device-to-device (D2D) communication underlying cellular networks is a promising technology to improve network resource utilization. In D2D-enabled cellular networks, interference generated by D2D communications is usually viewed as an obstacle to cellular communications. However, the authors presented a new perspective on the role of D2D interference by taking security issues into consideration. To considered a large-scale D2D-enabled cellular network with eavesdroppers overhearing cellular communications. Using stochastic geometry model such a network and analyzed the signal-to-interference plus-noise ratio (SINR) distributions, connection probabilities and secrecy probabilities of both the cellular and D2D links. They proposed two criteria for guaranteeing performances of secure cellular communications, namely the strong and weak performance guarantee criteria. Based on the analytical results of link characteristics and the design of optimal D2D link scheduling schemes are the two criteria respectively. Both analytical and numerical results show that the interference from D2D communications can enhance physical layer security of cellular communications and at the same time create extra transmission opportunities for D2D users.

H. Wang, X. Zhou, and M. Reed [15] studied the information-theoretic secrecy performance in large-scale cellular networks based on a stochastic geometric framework. The locations of both base stations and the mobile users are modeled as independent two-dimensional Poisson point processes. To considered two important features of cellular networks, namely, information exchange between base stations and cell association, to characterize their impact on the achievable secrecy rate of an arbitrary downlink transmission with a certain portion of the mobile users acting as potential eavesdroppers. In particular, tractable results are presented under diverse assumptions on the availability of eavesdroppers' location information at the serving base station, which captures the benefit from the exchange of the location information between base stations.

C. Cai, et al. [16] considered the transmission of a confidential message from a source to a destination in a decentralized wireless network in the presence of randomly distributed eavesdroppers. The source-destination pair can be potentially assisted by randomly distributed relays. The arbitrary relay is used to derive exact expressions of secure connection probability for both colluding and non-colluding eavesdroppers. To further obtain lower bound expressions on the secure connection probability, which are accurate when the eavesdropper density is small. By utilizing these lower bound expressions, to proposed a relay selection strategy to improve the secure connection probability. By analytically comparing the secure connection probability for direct transmission and relay transmission, to addressed the important problem of whether or not to relay and discuss the condition for relay transmission in terms of the relay density and source-destination distance.

C. Cai, et al. [17] illustrated the security failures of cryptographic protocols is the key to both patching existing protocols and designing future schemes. In this work, the authors investigated two recent proposals in the area of smart-card-based password authentication for security-critical real-time data access applications in hierarchical wireless sensor networks (HWSN). Firstly, to analyze an efficient and DoS-resistant user authentication scheme. This protocol is the first attempt to address the problems of user authentication in HWSN and only involves lightweight cryptographic primitives, such as one-way hash function and XOR operations, and thus it is claimed to be suitable for the resource-constrained HWSN environments. However, it actually has several security loop- holes being overlooked, and we show it is vulnerable to user anonymity violation attack, smart card security breach attack, sensor node capture attack and privileged insider attack, as well as its other practical pitfalls.

III. Conclusion and Future Work

The Dynamic Secure Networks with Probabilistic Graph Modeling and Linear Programming in wireless networks to be formalized, implemented, and evaluated a new probabilistic model for measuring the security threats in large enterprise networks. A selection of secure models in wireless network was discussed in the literature review; however, most of them suffer from large collision networks with inside and outside attacks. This survey shows the challenges that face the design of an efficient and effective secure protocol detection model for large wireless networks should be satisfied to design such models.

REFERENCES

1. K. Ingols, R. Lippmann, and K. Piwowarski, “Practical attack graph generation for network defense,” in Computer Security Applications Conference, 2006., 12 2006, pp. 121 –130.
2. S. Jajodia, S. Noel, and B. O’Berry, “Topological analysis of network attack vulnerability,” in Managing Cyber Threats: Issues, Approaches and Challanges, V. Kumar, J. Srivastava, and A. Lazarevic, Eds. Kluwer Academic Publisher, 2003, ch. 5.
3. L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An Accurate and Precise Malicious Node Exclusion Mechanism For Ad Hoc Networks," Ad Hoc Networks - Elsevier B.V., vol. 19, pp. 142–155, 2014.
4. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," 2070-1721, 2003.
5. J. Mo, M. Tao, Y. Liu, and R. Wang, “Secure beamforming for mimo two-way communications with an untrusted relay,” IEEE Trans. Signal Process., vol. 62, no. 9, pp. 2185–2199, May 2014.
6. Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physicallayer security in cooperative wireless networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
7. D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, “Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks,” IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 2067–2076, Dec. 2011.
8. A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, “Jamming-aware minimum energy routing in wireless networks,” in Proc. IEEE Int. Conf. Commun. (ICC), June 2014, pp. 2313–2318.
9. Z. Ding, K. Leung, D. Goeckel, and D. Towsley, “On the application of cooperative transmission to secrecy communications,” IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359–368, Feb. 2012.
10. X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” IEEE Trans. Wireless Commun., vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
11. M. Saad, “Joint optimal routing and power allocation for spectral efficiency in multi-hop wireless networks,” IEEE Trans. Wireless Commun., vol. 13, no. 5, pp. 2530–2539, May 2014.
12. C. Wang, H.-M.Wang, and X.-G. Xia, “Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks,” IEEE Trans. Wireless Commun., vol. 14, no. 2, pp. 589–605, Feb 2015.
13. J. Li, A. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
14. C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, “Interference exploitation in d2d-enabled cellular networks: A secrecy perspective,” IEEE Trans. Commun., vol. 63, no. 1, pp. 229–242, Jan. 2015.
15. H. Wang, X. Zhou, and M. Reed, “Physical layer security in cellular networks: A stochastic geometry approach,” IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 2776–2787, May 2013.
16. C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, “When does relay transmission give a more secure connection in wireless ad hoc networks?” IEEE Trans. Inf. Foren. Sec., vol. 9, no. 4, pp. 624–632, Apr. 2014
17. D. Wang and P. Wang, "Understanding Security Failures of Two-Factor Authentication Schemes For Real-Time Applications In Hierarchical Wireless Sensor Networks," Ad Hoc Networks - Elsevier B.V., vol. 20 pp. 1–15, 2014.