ISSN No. 0976-5697

Volume 7, No. 5, September-October 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY ON SECURE ROUTING IN MULTI-HOP WIRELESS NETWORK

A.Anitha M.sc (CT)
Research Scholar
Department of Computer Science
Kongunadu Arts and Science College
Coimbatore, Tamilnadu, India

Dr. S. Mythili MCA, M.Phil., Ph.D
Associate Professor and Head
Department of Information Technology
Kongunadu Arts and Science College,
Coimbatore, Tamilnadu, India

Abstract:Secure Routing is a fundamental networking function in every communication system, and multi-hop wireless networks are no exceptions. Attacking the routing service, achallenger can easily paralyses the operation of an entire network. The problem of traditional routing schemes relies on the possibility that the network is connected, that is, there is an end-to-end path between any source and any destination. Over the past, Secure Routing in Multi-hop Wireless Ad-hoc Networks techniques have been illustrated in this research. Itaims to present a surveyon secure routing protocol techniques in physical layer security, Secure routing with the default decode and forward strategy and cost of physical layer security in decentralized wireless networks.The researchwork also discuss about the relaying strategies in wireless ad hoc networks, secure connection path between the source and destination through the intermediate relay nodes and also about how the intermediate relay selection is been made and what algorithm and protocols are been implemented in order to achieve secure connection path. The secure connection path is said to be secured or unsecured only after analyzing about both the colluding eavesdroppers and non-colluding eavesdroppers. Hence, the research work also discuss about both type of eavesdroppers.The research presents a survey of the most significant opportunistic routing protocols for multi-hop wireless networks.

Keywords: Secure routing, multi-hop, wireless ad hoc networks, relay, eavesdroppers

I. INTRODUCTION

Network security is a fundamental issue of communication systems. For wireless networks, secure communication is more challenging due to the broadcast nature of wireless channels. The traditional approach for secure communication is to employ the cryptographic algorithms. Recently, physical layer security has emerged as a complementary technology to the cryptography-based method, which can achieve perfect secrecy by properly designing the encoder decoder of transceivers according to the channel conditions [1], [2].

The Wireless Ad Hoc Network (WANET) is a distributed type of wireless network. An ad hoc network classically refers to any set of networks where all devices have equal status. The features of wireless ad hoc network are as follows (i) the nodes are static(ii) network is connected where the existence of end-to-end path available (iii) the scalability improves due to distributed nature of wireless network type (iv)the transmission is been carried out via the multiple hops (v) it is infrastructure less, self-configuring, self-forming, self-healing network.

The research work discuss about the relaying strategies in wireless ad hoc networks, secure connection path between the source and destination through the intermediate relay nodes then how the intermediate relay selection is been made and what algorithm and protocols are been implemented in order to achieve secure connection path. The secure connection path is said to be secured or unsecured only after analyzing about both the colluding eavesdroppers and non-colluding eavesdroppers.

II. LITERATURE REVIEW

I. Csiszar and J. Korner [2] discussed two discrete memory less channels (DMC's) with a common input, it is desired to transmit private messages to receive 1 at R_1, and commonmessages to both receivers at rate R_0, while keeping receiver 2
as ignorant of the private messages as possible. Measuring ignorance by equivocation, a single-letter characterization is given bythe achievable triples (R_i, R_e, R_0) where R_e is the equivocation rate. Based on this channel ding result, the related source-channel matching problem is also settled. The authors considered a model for simultaneously broadcasting both messages for common use and confidential messages. For this model the authorshas characterized the achievable rates in terms of information quantities, so that the rate region is, in principle, computable. This is the commonly accepted criterion of a "solution" in multi-user Shannon theory. In some simple case the numerical results are readily obtained.

J. M, et.al[3] studied the secure beam forming design in a multiple-antenna three-node system where two source nodes exchange messages with the help of an untrusted relay node. The relay acts as both an essential signal forwarder and a potential eavesdropper. Both two-phase and three-phase two-way relay strategies are considered. The author's goal is to jointly optimize the source and relay beam formers for maximizing the secrecy sum rate of the two-way communications. They first derive the optimal relay beam former structures. Then, iterative algorithms are proposed to find source and relay beam formers jointly based on alternating optimization. The authors have also conducted the asymptotic analysis on the maximum secrecy sum-rate. Authors 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.

The authors concluded that the conventional two-way direct transmission is preferred when the relay power goes to zero. When the relay power approaches infinity and source powers approach zero, the three-phase two-way relay scheme performs best. Moreover, when all powers go to infinity, the two-phase two-way relay scheme has the best performance if signal alignment techniques are used, which also lowers the requirement of numbers of antennas at the source nodes for security.

Y. Zou, X. Wang, and W. Shen[4] 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. The author proposed the AF and DF based optimal relay selection (i.e., AF*b*ORS and DF*b*ORS) schemes to improve the wireless security against eavesdropping attack. For the purpose of comparison, and examined the traditional AF*b*ORS and DF*b*ORS schemes, denoted by T-AF*b*ORS and TDF*b*ORS, respectively. And also investigate a so-called multiple relay combining (MRC) framework and present the traditional AF and DF based MRC schemes, called T-AF*b*MRC and TDF*b*MRC, where multiple relays participate in forwarding the source signal to destination which then combines its received signals from the multiple relays. The work derives closed-form intercept probability expressions of the proposed AF*b*ORS and DF*b*ORS (i.e., P-AF*b*ORS and P-DF*b*ORS) as well as the T-AF*b*ORS, TDF*b*ORS, T-AF*b*MRC and T-DF*b*MRC schemes in the presence of eavesdropping attack. Further the conduct an asymptotic intercept probability analysis to evaluate the diversity order performance of relay selection schemes and show that no matter which relaying protocol is considered (i.e., AF and DF), the traditional and proposed optimal relay selection approaches bothachieve the diversity order *M* where *M* represents the number of relays.

D. Goeckel, et.al[5] discussed the secure transmission of information in wireless networks without knowledge of eavesdropper channels or locations are 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, is to 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 presented work of secure transmission information suggests a number of avenues for future research. Critical to the applicability of the results is an understanding of the rate at which the outage probabilities of the desired receivers and eavesdroppers converge to their asymptotic limits. A detailed study of such, while beyond the scope of the present work, is the most compelling future research direction. While considering the case of colluding eavesdroppers, as of interest when considering the information-theoretic secrecy scenario. The authors suggested the techniques which require an exponential tail of the probability density function of the random power gain caused by the fading.

A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, [6] 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. The percentage of energy saved by the proposed method with respect to a shortest path routing benchmark is evaluated. It is shown that the amount of energy saved, especially in terrestrial wireless networks with path-loss exponents greater than two, is substantial. The consideration of more sophisticated dynamic jammers with or without eavesdropping capabilities is an important topic for further research.

Z. Ding, K. Leung, D. Goeckel, and D. Towsley,[7] 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 by the authors, since it is animportant 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 the transmission power. The authorsintroducedthe 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. They focused on the secrecy communication scenario where all nodes are equipped with a single antenna. The outage performance of three schemes: the best relay scheme, the cooperative scheme using all qualified relays, and the MISO lower bound. As can be seen from the figure, the curves for the scheme using all qualified relays have the same slope as the ones for the MISO bound, which confirms that this cooperative scheme can achieve the diversity gain.

X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes[8] studied the throughput of large-scale decentralized wireless networks with physical layer security constraints. In particular, there is inquisitiveness 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. The study uses of a secrecy guard zone, which is shown to give a significant improvement on the throughput of networks with high security requirements.

This model of secrecy transmission capacity can be extended to analyze and design networks with other transmission techniques, medium access control protocols, and eavesdropping strategies in future work. Similar to other transmission capacity formulations, the main limitation of this model is that it only considers single-hop transmissions, while the communication between an arbitrary source-destination pair usually requires multiple hops. End-to-end throughput analysis of wireless networks with physical layer security requirements is still an open problem. Another limitation of the current model is the homogeneous Poisson distribution of nodes. The impact of eavesdropper distribution on secrecy throughput is an interesting problem to investigate.

III. CONCLUSION

The presented work is a state-of-the-art survey on Secure Routing in Multi-hop Wireless Ad-hoc Networks. The research work discussed about the existing techniques of physical layer security, Secrecy throughput maximization for *df* relay networks and Cost of physical layer security in decentralized wireless networks which has also been stated thelimitationsof the existing technique in terms of metrics as secure routing, quality of service, delay and security consumption. Through comprehensive analysis of secure routing issues in Wireless Ad-hoc network problem definitions to the previous techniques, a complete representation of the state-of-the-art on secure routing in multi-hop wireless ad-hoc network can be described.

IV. REFERENCES

[1] A. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.