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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A Survey on Confidential Multicasting in The Presence of Eavesdroppers

Duhita Pawar[1], Prof.Vina M. Lomte[2]

Student, Department of Computer Engineering RMD, Sinhgad School of Engineering Pune, India[1]

Professor, Department of Computer Engineering, RMD, Sinhgad School of Engineering Pune, India[2]

ABSTRACT: Confidentiality preserving is crucial task in multi hop wireless sensor network for multiple source and destination in the network. Authorization of intermediate node is important aspect multi-hop packet transmission with efficient utility maximization. It is necessary to design novel approach to optimal dynamic control which maintains flow control, routing and end to end packet authentication. In Proposed system researchers present the protocols for creating pair wise secrets between nodes in a wireless network, so that these secrets are secure from an eavesdropper. They first present a basic secret-agreement protocol for single-hop networks, where secrets are constructed using traffic exchanged between the nodes, and we show that under standard theoretical assumptions, our protocol is information-theoretically secure. Second, we propose a secret-agreement protocol for arbitrary, multi-hop networks that build on the basic protocol but also comprises design features for leveraging additional sources, that multi-hop offers, for secrecy.

KEYWORDS: Secret key generation, packet erasures, multi-hop key agreement, wireless networks.

I. INTRODUCTION

To develop an efficient secret data transmission technique. When the confidential data or information is transferred from source to the destination it is travelled from hop to hop and finally to the destination. But there is possibility that while the data packets are sent from source to destination they are overheard by some middle eavesdropper who compromises our data. The objective of this paper is to develop an efficient technique by using different algorithm to save the confidential data from eavesdropper. The problem of network control with confidential messages has been studied (as shall be discussed in the next section), in the past for the single-hop setting. The main additional challenges involved in generalizing this problem to multihop networks are dynamic end-to-end encoding and multipath routing. Standard dynamic control algorithms give control decisions in each time slot independently
by assuming time-scale separation, i.e., independent transmissions of subsequent slots .
The confidential message is encoded across many blocks, which implies that the time-scale involved in physical-layer resource allocation cannot be decomposed from the time scales involved in networklayer resource allocation, eliminating the time-scale separation assumption of standard dynamic control algorithms.

II. RESEARCH METHOD

Paper name: A network coding approach to energy efficient broadcasting: From theory to practice:-
In literature survey of this paper proposes that network coding allows to realize energy savings in a wireless ad-hoc network, when each node of the network is a source that wants to transmit information to all other nodes. Energy efficiency directly affects battery life and thus is a critical design parameter for wireless networks. In this paper researcher propose an implementable method for performing network coding in such a setting. They analyze theoretical cases in detail, and use the insights gained to propose a practical, fully distributed method for realistic wireless ad-hoc scenarios. [1]

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Paper name: A performance comparison study of ad hoc wireless multicast protocols:-
This paper investigates the performance of multicast routing protocols in wireless mobile ad hoc networks. An ad hoc network is composed of mobile nodes without the presence of a wired support infrastructure. In this environment, routing Multicasting protocols are faced with the challenge of producing multihop routes under host mobility and bandwidth constraints. In this study, researchers simulate a set of representative wireless ad hoc multicast protocols and evaluate them in various network scenarios. The relative strengths, weaknesses, and applicability of each multicast protocol to diverse situations are studied and discussed.[2]

Paper name: Exchanging pairwise secrets efficiently:-
This paper propose a simple secret-agreement protocol, where the wireless nodes keep exchanging bits until they have agreed on pairwise secrets that Eve cannot reconstruct with very high probability. It protocol relies on Eve as limited network presence (the fact that she cannot be located at an arbitrary number of points in the network at the same time), but assumes nothing about her computational capabilities. Researchers formally show that, under standard theoretical assumptions, our protocol is information-theoretically secure[3]

Paper name: Exploiting fountain codes for secure wireless delivery:-
In this paper, a secure delivery scheme that exploits fountain codes is analyzed. For fountain-coded transmission, the receivers have to obtain a sufficient number of fountain packets to recover the original data. Secure delivery can be achieved if the legitimate user receives enough fountain packets first. For this purpose, researchers utilize the independent channel fading of different users to ensure a higher packet reception rate at the destination. The channel fading is competent if the destination is known to have a better average channel condition than that of the eavesdropper; otherwise, transmit power control relative to the destination channel is employed.[4]

Paper name: On secure communication over wireless erasure networks:-
This paper studies the secrecy capacity of unicast communication in a wireless erasure network setting in the presence of a wire-tapper. From an information-theoretic setting of perfect secrecy, both upper bounds and achievable secrecy rates are presented. Secrecy capacity is determined in closed form for a class of broadcast constrained erasure networks[5]

Paper name: On the inherent security of linear network coding:-
In this paper, by targeting passive attackers, a new security protocol based on the inherent security of linear network coding is proposed .The probability of finding proper encoding vectors and the probability of protocol security assurance drastically increase as the code field size or the number of transmittable symbols increase, or as the attacker becomes more limited in accessing independent channels.[6]

Paper name: Secrecy capacities for multiterminal channel models:-
In this paper researchers generate the secret key for a set A of terminals of the noisy channel, with the remaining terminals (if any) cooperating in this task through their public communication. Single-letter characterizations of secrecy capacities are obtained for models in which secrecy is required from an eavesdropper that observes only the public communication and perhaps also a set of terminals disjoint from A . These capacities are shown to be achievable with non interactive public communication, the channel input terminal sending no public message and each output terminal sending at most one public message, not using randomization.[7]

Paper name: Secret key agreement by public discussion from common information:-
This paper suggest how to build cryptographic systems that are provably secure against enemies with unlimited computing power under realistic assumptions about the partial independence of the noise on the involved communication channels.[8]

Paper name: Secret key agreement by public discussion from common information:-
This paper introduces a set of low-complexity algorithms that when coupled with link layer re-transmission mechanisms, strengthen wireless communication security. The basic idea is to generate a series of secrets from

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

inevitable transmission errors and other random factors in wireless communications. Because these secrets are constantly extracted from the communication process in real-time, researchers call them dynamic secrets.[9]

Paper name: Secure wireless communication with dynamic secrets:-
This paper addresses the correlated erasure events across the two channels in a wiretap feedback framework. The intuitive notion that high correlation across channels reduces secrecy is shown through the complete characterization of the correlated channel scenario. Furthermore, it is shown that security Improvements are still achievable in the face of positive correlation by means of judicious physical layer design, even when the eavesdropper has a better channel than the legitimate receiver.[10]

Paper name: Physical layer security over cor-related erasure channels:-
In this paper researchers considered the downlink scheduling problem in multi queue multi-server systems under channel uncertainty. Two policies are proposed that make allocations based on predicted channel states .The first approach is an extension of the well known dynamic backpressure policy to the uncertain channel case. The second approach is a variant which improves the delay performance under light loads. The stability region of the system is characterized and first policy is argued to be the throughput optimal.[11]

Paper name: Information-theoretic secrecy for wireless networks:-
In this paper researchers summarize work on Information theoretically secure wireless relay network communication. In such communication the goal is to send the information between two special nodes where the secrecy is with respect to the class of the eavesdroppers. They develop achievable secrecy rates when authenticated relays which also help increasing secrecy rate by inserting noise into the network.[12]

Paper name:On the secrecy capacity of fading channels:- In this paper researchers con-
sider the secure transmission of information over an fading channel in the presence of an eavesdropper. The eavesdropper can be viewed as the wireless counterpart of Wyner as wire-tapper. The secrecy capacity of such system is characterized under the assumption of asymptotically long coherence inter vals. They analyze the full Channel State Information (CSI) case where the transmitter has the access to channel gains of the legitimate receiver and eavesdropper and main CSI scenario where only the legitimate receiver channel gain is known at the transmitter. In each case the secrecy capacity is obtained along with the optimal power and the rate allocation strategies.[13]

Paper name: Optimal Congestion Control and Routing for Multipath Networks with Random Losses:-
Researchers consider optimal congestion control and routing schemes for multipath networks with non-congestion related packet losses which may be caused by for example, errors on links on routes and develop a relaxed multipath network utility maximization problem. They present the primal algorithm which is known to be globally stable in the absence of round trip delays .When the round trip delays are considered decentralized ,sufficient conditions for the local stability of algorithm are proposed in both the continuous time and discrete time forms. Finally, a window flow control mechanis is presented which approximate the optimum of the multipath network utility maximization model.[14]

Paper name: On cooperative wireless network secrecy:-
Given that wireless communication occurs in a shared and inherently broadcast medium, the transmissions are vulnerable to the undesired eavesdropping. This occurs even when a point-to-point communication is sought So the fundamental question is whether we can utilize the wireless channel properties to establish secrecy. In this paper Researchers consider the secret communication between the two special nodes network with authenticated relays: the message communicated to destination is to be kept information theoretically secret from any eavesdropper within the class. Since the transmissions are broadcast and confidential Multicasting in the presence of eavesdroppers interfere with each other, complex signal interactions occur.[15]

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

III. EXISTING SYSTEM

According to literature survey we came to know that there are certain constraints and limitations of the existing system.In existing systems hop to hop communication in wireless sensor network considered to provable for vulnerability ofdata transfer. Due to hop to hop communication increased cost for packet transmission.Existing system uses security mechanism as node to node authentication among network resources Hop to hop identity of intermediate node compromise security threats. To avoid security threat they uses digital signature authentication at node level for communication or packet transmission. In existing system message transmission is done through all neighbors betweensource and destination nodes, which result in over hearing and increase overhead between nodes. Since the pioneering work of Wyner, there has been a wide interest on the variations of the wiretap channel and how to provide secrecy in various multiuser and network information theoretic scenarios, mainly under the single hop setting. To give a few examples on the single hop setting, opportunistic secrecy was introduced, which allows for the exploitation of channel variations due to fading to achieve secrecy, even when the eavesdropper has a higher average signal-tonoise ratio. Achieving delay-limited secrecy and outage capacity of the wiretap channel were studied in. The use of multiple antennas for secrecy under a variety of assumptions has been considered in. Multiuser communication with secrecy using cooperative jamming and relaying in the presence of eavesdropper was studied . In the multihop setting, studies the secrecy capacity scaling problem. Exploitation of path diversity in order to achieve secrecy from external eavesdroppers is studied in and for secrecy via mobility. In a method is given that modifies any given linear network code into a new code that is secure requiring a large field size. Later, generalized and simplified the method in, and showed that the problem of making a linear network code secure is equivalent to the problem of finding a linear code with certain generalized distance properties. Along the same lines, investigates secure communication over wireline networks where a node can observe one of an arbitrarily selected collection of secure link sets. In a different notion of security referred to as packet-level security is used, where it is sufficient that the eavesdropper does not correctly decode the message, i.e., it does not guarantee full equivocation. In addition, assumes availability of private secure channels between source and destination nodes that are not accessible to the eavesdropper, but are more costly. The objective is to minimize the use of private channels subject to a required level of security in order to understand the trade-off between the security level and the cost incurred by security. Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques.There has been only a few studies on wireless network control and protocol design with secrecy/confidentiality as aconstraint on the transmitted information. Therefore, our understanding of the interplay between the confidentiality requirements and the critical functionalities of wireless networks, such as scheduling, routing, and congestion control remains limited In addition, assumes availability of private secure channels between source and destination nodes that are not accessible to the eavesdropper, but are more costly. The objective is to minimize the use of private channels subject to a required level of security in order to understand the trade-off between the security level and the cost incurred by security. Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques. There has been only a few studies on wireless network control and protocol design with secrecy/confidentiality as a constraint on the transmitted information. Therefore, our understanding of the interplay between the confidentiality requirements and the critical functionalities of wireless networks, such as scheduling, routing, and congestion control remains limited.

IV. APPLICATIONS

Space is another characteristic of wireless networking. Wireless networks offer many advantages when it comes to difficult-to-wire areas trying to communicate such as across a street or river, a warehouse on the other side of the premise or buildings that are physically separated but operate as one. Wireless networks allow for users to designate a certain space which the network will be able to communicate with other devices through that network. Space is also created in homes as a result of eliminating clutters of wiring. This technology allows for an alternative to installing physical network mediums such as TPs, coaxes, or fiberoptics, which can also be expensive. The industry accepts a handful of different wireless technologies. Each wireless technology is defined by a standard that describes unique functions at both the Physical and the Data Link layers of the OSI Model. These standards differ in their specified signalling methods, geographic ranges, and frequency usages, among other things. Such differences can make certain technologies better suited to home networks and others better suited to network larger organizations.

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

V. CONCLUSION

Researchers have presented two protocols for enabling a group of n wireless nodes to create pairwise secrets, in the presence of a passive adversary, with limited network presence, without assuming anything about her computational and memory capabilities. Their basic secret-agreement protocol operates in single-hop networks, it is information-theoretically secure and leverages broadcast to create secrets simultaneously between all terminal pairs. Their protocol for arbitrary, multi-hop networks, builds on the basic protocol and includes new designs, e.g., a custom packet dissemination protocol, to leverage the benefits of multi-hop for secrecy generation. On the practical side, they evaluated our protocols through testbed experimentation and extensive simulations, and they showed that, both on single-hop and multi-hop networks, it is feasible to generate secrets at non-negligible rates. Their results motivate us to investigate further the robustness of their protocols, under the presence of adversaries with increasing network presence (multiple antennas, collaborating Eves etc.

ACKNOWLEDGEMENTS

I take this chance to express my appreciation to my guide and Head of the Department of Computer Engineering, RMDSSOE, Prof. Vina M. Lomte for her kind cooperation and guidance during the entire research work. I would also like to thank our Principal and Management for providing lab and other facilities.

REFERENCES

[1] C. Fragouli, J. Widmer, and J.-Y. Le Boudec, aA network coding approach to energy efficient ˆ broadcasting: From theory to practice,a in Proc. INFOCOM, 2006, pp

[2] S.-J. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia, aA performance comparison study of ad hoc ˆ wireless multicast protocols,a in Proc. INFOCOM, 2000, pp. 565 ˆ a574.

[3] Safaka, C. Fragouli, K. Argyraki, and S. Diggavi, aExchanging pairwise secrets efficiently, ˆ a in ˆ Proc. IEEE INFOCOM, Apr. 2013, pp. 2265a2273. ˆ

[4] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, aExploiting fountain codes for secure wireless ˆ delivery,a IEEE Commun. Lett., vol. 18, no. 5, pp. 777 ˆ a780, May 2014. ˆ

[5] A. Mills, B. Smith, T. C. Clancy, E. Soljanin, and S. Vishwanath, aOn secure communication over ˆ wireless erasure networks,a in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2008, pp. 161 ˆ a165. ˆ

[6] M. Adeli and H. Liu, aOn the inherent security of linear network coding, ˆ a IEEE Commun. Lett., ˆ vol. 17, no. 8, pp. 1668a1671, Aug. 2013. ˆ

[7] I. Csiszar and P. Narayan, aSecrecy capacities for multiterminal channel models, ˆ a IEEE Trans. ˆ Inf. Theory, vol. 54, no. 6, pp. 2437a2452, Jun. 2008. ˆ

[8] U. M. Maurer, aSecret key agreement by public discussion from common information, ˆ a IEEE ˆ Trans. Inf. Theory, vol. 39, no. 3, pp. 733a742, May 1993. ˆ

[9] S. Xiao, W. Gong, and D. Towsley, aSecure wireless communication with dynamic secrets, ˆ a in ˆ Proc. INFOCOM, 2010, pp. 1a9. ˆ

[10] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, aPhysicallayer security over cor- ˆ related erasure channels,a in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 888 ˆ a892. ˆ

[11] C. Manikandan, S. Bhashyam, and R. Sundaresan, EaCross-layer scheduling with infrequent ¨ channel and queue measurements,Ea IEEE Trans. Wireless Commun., vol. 8, no. 12, pp. ¨ 5737Ea5742, Dec. 2009

[12] E. Peron, EaInformation-theoretic secrecy for wireless networks, ¨ Ea Ph.D. dissertation, EPFL, ¨ Lausanne, Switzerland, 2009

[13] P. K. Gopala, L. Lai, and H. E. Gamal, EaOn the secrecy capacity of fading channels, ¨ Ea IEEE ¨ Trans. Inf. Theory, vol. 54, no. 10, pp. 4687Ea4698, Oct. 2008. ¨

[14] Shiyong LI, Wei SUNEa, Yaming ZHANG, Yehua CHEN School of Economics and Man- ¨ agement, Yanshan University Qinhuangdao 066004, China e-mail: shiyongli@ysu.edu.cn, wsun@ysu.edu.cn, yaming99@ysu.edu.cn,

[15] E. Perron, S. Diggavi, and E. Telatar, EaOn cooperative wireless network secrecy, ¨ Ea in Proc. ¨ IEEE INFOCOM, Rio de Janeiro, Brazil, Sep. 2009, vol. 4, pp. 1935Ea1943