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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Network Security for Confidential Multi-Hop Communications

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

Dept. of Computer, RMD Shingad School of Engineering, Pune, India

ABSTRACT: In wireless sensor network messages are transferred between multiple source and destinationpairs cooperatively such way that multi-hop packet transmission is used. These data packets are transferred from intermediate node to sink node by forwarding packet to destination nodes. Where every node overhead transmission near neighbor node. To avoid this researchers propose novel approach with efficientrouting protocol i.e. shortest path routing and distributed node routing algorithm. Proposed work also focuses on Automatic Repeat Request and Deterministic Network coding. They propagate this work by end to end message encoding mechanism. To enhance node security pairwise key generation is used, In which paired communicating node is assigned with pair key to make secure communication end to end.

I. INTRODUCTION

Researchers have considered the problem of resource allocation and control of multi-hopnetworks in which the multiple source-destination pairs do communicate confidential messages, to be kept confidential from the intermediate nodes. Theyproposed the problem as that of network utility maximization into which an additional quality of service constraint, confidentiality is incorporated. They develop a simple yet provably optimal dynamic control algorithm that combines flow control, routing and end-to-end secrecy-encoding. In order to achieve the confidentiality, this scheme exploits multipath diversity and temporal diversity due to channel variability. This scheme of end-to-end dynamic encoding encodes confidential messages across multiple packets, to be combined at a ultimate destination for recovery. They first of all develop an optimal dynamic policy for the case in which the number of blocks across which secrecy encoding is performed is asymptotically large. Again, they consider the encoding across a finite number of packets, which eliminates the possibility of achieving perfect secrecy. Researchers has developed the dynamic policy to choose the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy requirements. From numerical analysis, they observe that proposed scheme approaches the optimal rates asymptotically with the increasing block size. Finally, they address the consequences of practical implementation issues such as infrequent queue updates and de-centralized scheduling. They demonstrate the efficiency of the policies by numerical studies under various network conditions

II. RESEARCH METHOD

Researchers considered an issue of secure transmissions in the delivered while keeping it secure from an eavesdropper. Two transmissions schemes were considered, a simple baseline Automatic Repeat Request scheme and the one based on deterministic Network Coding. The results shows that the tradeoff between achieving a certain security level and the cost incurred. Also, the results shows that Network Coding considerably reduces security cost compared to the case when the simple Automatic Repeat Request is used. Overall, this work constitutes a modest but important step towards resolving any important problem of wireless networking that combines security issues with performance costs and the distributed operation.[1] To use cooperating relays to improve performance of the secure wireless communications in the presence of one or more eavesdroppers. The three cooperative schemes have been considered: decode-and-forward, amplify- and-forward and cooperative jamming. Researchers have considered two practical design problems, i.e., allocate the transmit power at source and relays and determine the relay weights in order to maximize the achievable secrecy rate subject to the transmit power constraint or minimize the total transmit power They have proposed designs for one and more eavesdroppers. [2]Researchers have addressed the secrecy capacity of wire-line networks where different links have different capacities and restricted wiretapping sets. For the case of networks with equal capacity

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

links where any links can be wiretapped, secrecy capacity is given by a cut-set bound if random keys are injected at the source, whether or not communicating users have information about the choice of the wiretap set. On the contrary, Researchers have shown that this rate is unachievable in general in the case of unknown wiretap sets or unequal capacity links, even if non-source nodes can generate randomness.[3] .This paper researcher proposes packet bit randomization for adding noise to original packet transmission. Securing the network does not entail a loss in the per-node throughput. The achievability argument is based on a novel multi-hop forwarding scheme where randomization is added in every hop to ensure maximal ambiguity at the eavesdropper[4] This paper focuses on role of such arrays in a less explored aspect of wireless systems, enhancing security. Specifically, Researchers develop and optimize physical layer techniques for using multiple antennas to protect digital transmissions from the potential eavesdroppers and analyze resulting performance characteristics. The natural framework for the protecting information at the physical layer is so-called wiretap channel introduced by Wyner and associated notion of the secrecy capacity. In the basic wiretap channel, there are three terminals, one sender, one receiver, and one eavesdropper. [5] In this paper, researchers obtained the achievable privacy rate region of single- and multi-user wireless systems using opportunistic scheduling when full channel state information of neighbors was available. Then, researchers described the cross-layer dynamic algorithm which works without the prior distribution of channel gains, and state a theorem shows that the algorithm achieves utility arbitrarily close to the achievable optimal utility. This simulation results also verifies that efficacy of the algorithm. As a future direction, researchers will consider the case when partial channel state information is available at each node, and the researchers will also consider scheduling in the downlink.[6] Researchers design a wireless communication system that achieves constant bit rate data transmission over the block fading channel, which is secure from an eavesdropper that listens to the transmitter over another independent block fading channel. By introducing the private key queues at both the transmitter and the receiver, researchers can exploit times at which main channel is favorable over eavesdropper channel to transmit some random private key bits along with data bits. These key bits are stored in a separate key queue at the transmitter as well as the receiver, and are utilized to secure data bits, whenever the channel conditions favor the eavesdropper. When main channel has the worse channel gain than eavesdropper, by consuming shared keys transmitter can confuse the eavesdropper, despite the limited main-channel rate.[7] Researchers address an important problem of the secure communication in a wireless network in the presence of eavesdroppers. Researchers present achievable scaling results on the rate of information that can be securely carried in a network, when the size of the network becomes large. In contrast to most of the previous work in this area, they assume the locations of the eavesdroppers are unknown. Compared to previous works that consider unknown eavesdropper locations, our construction can achieve the same secure throughput scaling while tolerating a significantly higher number of eavesdroppers.[8] Researchers investigate the use of message-passing algorithmsfor the problem of finding the max-weight independent setin a graph. They show that any problem of map estimation forprobability distributions over finite domains can be reduced toan max-weight independent set problem. They believe this reduction will yield newinsights and algorithms for map estimation.[9] Secure network coding has been introduced to prevent information from being leaked to adversaries. The investigation of performance bounds on numbers of the source symbols and random symbols are two fundamental research problems. For important case that each wiretap-set with cardinality not larger than r, Researchers proposed the coding scheme, which is optimal in the sense of maximizing the number of source Symbols and at same time minimizing the number of random symbols .They further study Achievable lower bound on number of random key and show that it just depends on the security constraint, and particularly, is independent to the information amount for transmission. This implies that when the number of transmitted source messages changes, They cannot reduce number of random key to keep the same security level [10]. 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] 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 "destination node" and "Source Node" in a memory less network with the authenticated relays, 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] In this paper researchers consider 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's wire-tapper. The secrecy

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

capacity of such system is characterized under the assumption of asymptotically long coherence intervals. 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] Researchers consider optimal congestion control and routing schemes for multipathnetworks with noncongestion related packet losses which may be caused by for example, errorson links on routes and develop a relaxed multipath network utility maximization problem. They present the primal algorithm which is known to be globally stablein the absence of round trip delays .When the round trip delays are considered decentralized ,sufficientconditions for the local stability of algorithm are proposed in both the continuous time and discrete timeforms. Finally, a window flow control mechanism is presented which approximate theoptimum of the multipath network utility maximization model..[14] 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 “source node” and “destination node” in the wireless 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 interfere with each other, complex signal interactions occur.[15]

III. COMPARITIVE STUDY OF VARIOUS CRYPTOGRAPHY ALGORITHMS

PARAMETERS	AES	DES	RSA	DIFFIE-HELLMAN
DEVELOPER	Vincent Rijmen and Joan Daemen in Belgium NIST	IBM	Rivest, Adi Shamir and Leonard adleman	whitfielddiffie and martin hellman
YEAR	2000	1977	1977	1976
KEY SIZE	128, 192 or 256 Bits	56 Bits	>1024bits	uses key exchange management
BLOCK SIZE	128, 192 or 256bits	64bits	Depends on key size	64bits
ROUNDS	10,12 or 14	16	1 round for each message	14
CYPHER TYPE	Rijndael cipher	Block cipher	Block cipher	symmetric key cipher
NETWORK TYPE	Feistel network	Feistel network	Common network	Common network
SECURITY ATTACK	Chosen plain attack	Brute force attack	Timing attack	Eavesdropping
MERITS	More secure and faster in both hardware and software	No real weakness has been found	Uses the public key and provides security to digital signatures that cannot be repudiated	Security factors in solving discrete algorithm is very challenging, the shared key is never itself transmitted over the channel
DEMERITS	Needs more processing	Possibility to break the encrypted code in DES	Speed is comparatively low	Lack of authentication

Table 1: Comparative Study of Various Cryptography Algorithms

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

IV. EXISTING APPROACH AND ITS DISADVANTAGES

In existing hop to hop communication in wireless sensor network considered to succumb for vulnerability of data transmission. Due to hop by 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 neighbor between source and destination nodes, which result in over hearing and increase overhead between nodes. Also it leads to compromised node communication in wireless sensor communication

V. CONCLUSION

Proposed work mitigate overhead forced by the updates transmitted to the scheduler. To avoid that, researchers implement unscheduled queue update algorithm, where users updates their queue length information periodically. They show that this algorithm again approaches the optimal solution in the expense of increasing average queue lengths. Then, they implement distributed version of dynamic control algorithms, where the scheduler decision is given according to local information available to each node. The simulation results show that the reduction in confidentiality rate due to usage of distributed algorithm is very less.

ACKNOWLEDGEMENTS

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Vina M. Lomte Head of Department, RMDSSOE (Computer Dept.) for her kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my Survey Paper.

REFERENCES

[1] N. Abuzainab and A. Ephremides, "Secure distributed information exchange," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1126–1135, Feb. 2014.
[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 4033–4039, Mar. 2010.
[3] T. Cui, T. Ho, and J. Kliewer, "On secure network coding with nonuniform or restricted wiretap sets," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 166–176, Jan. 2013.
[4] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.
[5] A. Khisti and G. W. Wornel, "Secure transmissions with multiple antennas:
The misome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3014, July 2010.
[6] C. E. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," *IEEE/ACM Trans. Netw.*, vol. 21, no. 1, pp. 324–337, Feb. 2013.
[7] O. Gungor, J. Tan, C. E. Koksal, H. E. Gamal, and N. B. Shroff, "Joint power and secret key queue management for delay limited secure communication," presented at the IEEE INFOCOM 2010, San Diego, CA, USA, Mar. 2010.
[8] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 1152–1160.
[9] S. Sanghavi, D. Shah, and A. Willsky, "Message-passing for maximum weight independent set," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4822–4834, Nov. 2009.
[10] J. Feldman, T. Malkin, R. Servedio, and C. Stein, "On the capacity of secure network coding," presented at the Allerton Conf. Commun., Contr., Comput., Monticello, IL, USA, Sep. 2004.
[11]C. Manikandan, S. Bhashyam, and R. Sundaresan, "Cross-layer scheduling with infrequent channel and queue measurements," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5737–5742, Dec. 2009.
[12] E. Peron, "Information-theoretic secrecy for wireless networks," Ph.D. dissertation, EPFL, Lausanne, Switzerland, 2009
[13] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[14]Shiyong LI, Wei SUN∗, Yaming ZHANG, Yehua CHEN School of Economics and Management, Yanshan UniversityQinhuangdao 066004, Chinae-mail: shiyongli@ysu.edu.cn, wsun@ysu.edu.cn, yaming99@ysu.edu.cn,
[15] E. Perron, S. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Sep. 2009, vol. 4, pp. 1935–1943