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 9, September 2016

Dynamic Confidentiality Authentication at Multi Hop Communication

Jayshri B. Patil[1], G.R.Shinde[2]

Student, Department of Computer, Smt Kashibai Navale College of Engineering, Pune (SKNCOE), Savitribai Phule Pune University Pune India.[1]

Professor, Department of Computer, Smt Kashibai Navale College of Engineering, Pune (SKNCOE), Savitribai Phule Pune University 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 multihop packet transmission with efficient utility maximization. It is necessary todesign novel approach to optimal dynamic control whichmaintains flow control, routing and end to end packet authentication. In proposed system multipath confidentiality preservation uses multipath diversity and temporal diversity of channel variability. In this study dynamic encoding scheme encodes confidential messages across multiple packets are combined at the ultimate destination for recovery. This work show dynamic policy for number block of original packet security. This scheme follows optimal rates with increasing block size. Additionally system resolves the consequences of practical implementation issues such as infrequent queue updates and de-centralized scheduling.

KEYWORDS: Mutual Nodes, Noise bit, Diamond Network, Multi-Hop Network.

I. INTRODUCTION

In multi hop packet transmission Confidentiality of intermediate nodes for communication is to be considered, so that data sent to a node is not shared by any other node. Also in which confidentiality is not necessary, it may be not secure to consider that nodes will always remain uncompromised. Keeping different node's information confidential can be viewed as a precaution to avoid a captured node from accessing information from other uncaptured nodes. In a multi hop network, as data packets are transferred, intermediate nodes get all or part of the data through directly forwarding data packets the transmission of nearby nodes, when transferring confidential messages. In this paper, I build efficient algorithms for confidential multiuser communication over multi hop wireless networks without the source-destination pairs having to share any secret key a priori. The metric I use to measure the confidentiality is the mutual information leakage rate to the relay nodes, i.e., the equivocation rate. I require this rate to be arbitrarily small with high probability and impose this in the resource allocation problem via an additional constraint.

To provide the basic intuition behind our approaches andhow the source nodes can achieve confidentiality from the relaynodes, consider the following simple example of a diamond network given in Fig.1. Let the source node have a single bitof information to be transmitted to the destination node, with*perfect secrecy* (with 0 mutual information leaked) from therelay node. The issue is that the source cannot transmitthis bit directly over one of the possible paths, violating the confidentialityconstraint. This problem can be solved by adding random noise(i.e., randomization bit) on the information bit, and sendingthe noise and the noise corrupted message over different paths,which can then be combined at the destination. Note that with the information available to the relay nodes,there is no way that they can make an educated guess aboutthe information bit, since they have *zero* mutual information. Hiding information from the other nodes can be made possibleby a careful design of end-to-end coding, data routing on topof other network mechanisms, flow control and scheduling inorder for an efficient resource utilization

DOI: 10.15680/IJIRCCE.2016. 0409169

II. LITERATURE SURVEY

The paper presented by the YunusSarikaya, C. EmreKoksal April 2016 provides us with the details of how the resource allocation problem affect the network performance, confidentiality problem of intermediate node, dynamic control algorithm for a given encoding rateand we prove that our algorithm achieves utility arbitrarily closeto the maximum achievable utility [1].

The paper presented by Tao Cui, TraceyHo, JörgKlieIr Jan 2013 gives the idea of Networks with unequal link capacities where a wiretapper can wiretap any subset of links, or networks where only a subset of links can be wiretapped. From this how the Secrecy rate is achievableFor the case of known but not unknown wiretap set as we know Determining the secrecy capacity is an NP-hard problem[2].

In the paper presented by AshishKhisti, Gregory W. WornellJuly 2010 proposed a masked beamforming scheme that radiates poIrisotropically in all directions and show that it attains near-optimal performance in the high SNR regime. Characterize the secrecy capacity in terms of generalized eigenvalues when the sender and eavesdropper have multiple antennas.The role of multiple antennas for secure communication is investigated within the framework of Wyner'swiretapchannel.[3].

O. OzanKoyluoglu, Can EmreKoksal, Hesham El Gamal May 2010. In this paper,the scaling behavior of the capacity of wireless networks under secrecy constraints and For extended networks with the path loss model is presented. A uniform rate per user is considered in this work.A path lossmodel is considered, where the legitimate and eavesdropper nodes are assumed to be placed according to Poisson point processes with intensities.[4]

The paper presented by N. Abuzainab and A. Ephremides Feb 2014, proposed scheme that Utilize private and public channels and wish to minimize the use of the (more expensive) private channel subject to a required level of security.Two transmissions schemes, a simple baseline ARQ scheme and the based on deterministic Network Coding can be considered for the proposed work.[5]

Lun Dong, Zhu Han, Athina P. Petropulu, H. Vincent Poor Mar 2010, In this paper,Use cooperating relays to improve the performance of secure wireless communications in the presence of one or more eavesdroppers. Three cooperativeschemes have been considered: decode-and-forward, amplify-and-forward and cooperative jamming. Conclusion, Physical (PHY) layer security approaches for wireless communications can prevent eavesdropping without upper layerdata encryption.[6].

C. EmreKoksal Feb 2013 presented that The secrecy constraint enforces an arbitrarily low mutual information leakage from the source to every node in the network,except for the sink node. I first obtain the achievable rate region for the problem for single- and multiuser systems assuming that the nodes have full channel state information (CSI) of their neighbors .In this paper, I studied the achievable private and openInformation rate regions of single- and multiuser wireless networks with node scheduling[7].

Qizhong Yao. In this paper, author introduced the concept of delay-aware energy balancing by minimizing the average transmission delay while taking into account the issue of unbalanced harvested energy distribution. Every UE first harvests the RF energy emitted by the AP and then sends data to the AP directly or via other UEs acting as relays in a time multiplexingmanner[8].

AbhijeetBhorkar, IEEE 2015 Each packet transmission can be overheard by a random subset of receivernodes among which the next relay is selected opportunistically. The main challenge in the design of minimum-delay routing policies is balancing the trade-off betIen routing the packets along the shortest paths to the destination and distributing the traffic according to the maximum backpressure. In this paper key points are 1.Congestion measure Implementation,2.LyapunovAnalysis , 3.Opportunistic Routing [9].

Yi Gao. This paper presents Pathfinder, a robust path reconstruction method against packet losses as as routing dynamics. At the node side, Pathfinder exploits temporal correlation between a set of packet paths and efficiently compressesthe path information using path difference.In this paper Wireless Sensor Networks, 1. Measurement 2.Path Reconstruction methodology is given.[10].

Ahmed E.A.A. Abdulla July 2012. In this paper author proposed Hybrid Multi-hop routing (HYMN) algorithm, which is a hybrid of the two contemporary multi-hop routing algorithm architectures, namely, flat multi hop routing that utilizes efficient transmission distances, and hierarchical multi-hop routing algorithms that capitalizes on data aggregation. In this paper focus is given on Wireless sensor Networks, Energy hole problem, Sink node Isolation [11].

SanghitaBhattacharyaa, SubhansuBandyopadhyayb 2012, In this paper author considered interference, transmission power and reception power of nodes asmetrics to derive a good quality routing path for delivering the packets from source to destination. Designed Protocol minimizes the total energy consumption of routing path from source to destination and balancesload among the nodes. For a given source to destination pair in the network, there may exist more than onerouting paths. Selecting a low interference energy efficient routing path gives a good balance between theinterference and energy utilization. Designed algorithm selects the low interference energy efficient path amongall the paths for a given source destination node pair [12].

A. Eryilmaz, R. Srikant Apr 2015, Authors studied the problem of stable scheduling for a classof wireless networks. Their goal is to stabilize the queues holdinginformation to be transmitted over a fading channel. Few assumptionsare made on the arrival process statistics other than the assumptionthat their mean values lie within the capacity region andthat they satisfy a version of the law of large numbers. They provethat, for any mean arrival rate that lies in the capacity region, thequeues will be stable under our policy. Moreover, show that it iseasy to incorporate imperfect queue length information and otherapproximations that can simplify the implementation of our policy.Presented conditions on scheduling policies thatguarantee stability for a large class of arrival and channelmodels.[13].

C. Manikandan, S. BhashyamDec 2009, The downlink scheduling problem in multi-queuemulti-server systems under channel uncertainty is considered.Two policies that make allocations based on predicted channelstates are proposed. The first is an extension of the well-knowndynamic backpressure policy to the uncertain channel case. Thesecond is a variant that improves delay performance underlight loads. The stability region of the system is characterized and the first policy is argued to be throughput optimal [14].

III. PROPOSED SYSTEM APPROACH

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 of data transfer. Due to hop to hop communication increased cost for packet transmission.Existing system uses security mechanism as node to node authentication among network resourcesHop 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 between source and destination nodes, which result in over hearing and increase overhead between nodes.

So from this **gap analysis**we come to know that there are some requirements which has to be considered to design the efficient system. So in proposed system we will provide that requirements:

In Proposed system we will design a optimal dynamic policy for the case in which the number of blocks across which secrecy encoding is performed is asymptotically large. Next, We consider encoding across a finite number of packets, which eliminates the possibility of achieving perfect secrecy. For this case, We will develop a dynamic policy to choose the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy outage requirements. Many important issues are considered in proposed system. In particular

a) To achieve confidentiality, one needs to encode blocks ofinformation across multiple packets. We develop a noveladaptive end-to-end encoding scheme, that takes certainobservations from the network and chooses the appropriatecode rate to maintain confidentiality for each blockof data.

b) In a multihop network, each node possibly overhears thetransmission of a packet multiple times as it is transmittedover multiple hops. We take into account such accumulationof information over multiple transmissions. Thus, weneed to go beyond the scenario given in Fig. 1, in whichthe paths are disjoint and each intermediate node has onlyone path crossing.

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 9, September 2016

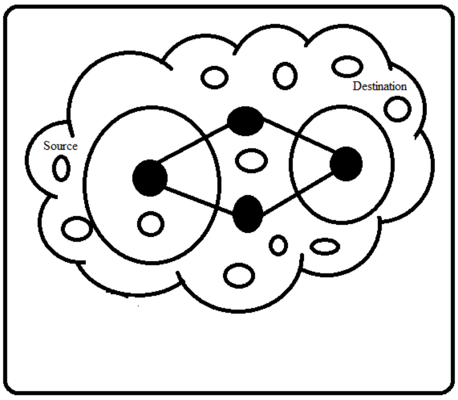

Fig 1. System Architecture

c) We combine a variety of strategies developed in thecontext of information theoretic secrecy with basic networkingmechanisms such as flow control and routing.Such a unifying framework is non-existent in the literatureas it pertains to multihop information transmission.For that purpose, we model the entire problem as that of anetwork utility maximization, in which confidentiality isincorporated as an additional constraint and develop theassociated dynamic flow control, routing, and schedulingmechanisms.

d) We take into account wireless channel variations in ourscheduling and routing policies as well as end-to-endencoding scheme for confidentiality. For that purpose,we assume that transmitters have perfect *instantaneous*channel state information (CSI) of their own channels.

IV. CONCLUSION

In this paper, We considered the problem of resource allocation in wireless multi-hop networks . All intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. So in order to maintain confidentiality end to end encoding with routing and flow control technique is incorporated. Additional constraint of security is considered and proposed dynamic network control algorithm. Proposed work mitigate overhead forced by the updates transmitted to the scheduler. To avoid that, Implement scheduled queue update algorithm, where users updates their queue length information periodically. We show that this algorithm again approaches the optimal solution in the expenseof increasing average queue lengths. Then, implement distributed version of dynamic control algorithms, where the scheduler decision is given according to local information available to each node.

REFERENCES

[1] YunusSarikaya, C. EmreKoksal, *Senior Member, IEEE*, and OzgurErcetin, " Dynamic Network Control for ConfidentialMulti-Hop Communications" , IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 24, NO. 2, APRIL 2016

[2] T. Cui, T. Ho, and J. KlieIr, "On secure network coding with nonuniform or restricted wiretap sets," IEEE Trans. Inf. Theory, vol. 59, no. 1, pp. 166–176, Jan. 2013.

[3] A. Khisti and G. W. Wornel, "Secure transmissions with multiple antennas:Themisome wiretap channel," IEEE Trans. Inf. Theory, vol.56, no. 7, pp. 3088–3014, July 2010.

[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] N. Abuzainab and A. Ephremides, "Secure distributed information exchange," IEEE Trans. Inf. Theory, vol. 60, no. 2, pp. 1126–1135, Feb. 2014.

[6] 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

[7] 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.

[8]C. EmreKoksal "Control of Wireless Networks With Secrecy" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 1, FEBRUARY 2013

[9] AbhijeetBhorkar "Opportunistic Routing With Congestion Diversity in Wireless Ad Hoc Networks" IEEE/ACM TRANSACTIONS ON NETWORKING1063-6692 © 2015 IEEE

[10]Yi Gao "Towards Reconstructing Routing Paths in Large Scale Sensor Networks" 10.1109/TC.2015.2417564, IEEE Transactions on Computers

[11] Ahmed E.A.A. Abdulla "HYMN: A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 11, NO. 7, JULY 2012

[12] SanghitaBhattacharyaa, SubhansuBandyopadhyayb, "An Interference Aware Minimum Energy Routing Protocol forWireless Networks Considering Transmission and ReceptionPower of Nodes", Procedia Technology 4 (2012) 1 – 8, 2212-0173,C3IT-2012

[13] A. Eryilmaz, R. Srikant, and J. R. Perkins, "Stable scheduling policiesfor fading wireless channels," *IEEE Trans. Inf. Theory*, vol. 13, no. 2,pp. 411–424, Apr. 2005.

[14] C. Manikandan, S. Bhashyam, and R. Sundaresan, "Cross-layer schedulingwith infrequent channel and queue measurements," *IEEE Trans.Wireless Commun.*, vol. 8, no. 12, pp. 5737–5742, Dec. 2009.