Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhancing Channel Bandwidth with Authentication in MANET Utility Function

S.Vinothkumar*
PG Scholar
SNS College of Engineering, Coimbatore
India

S.Boopathy
Assistant Professor
SNS College of Engineering, Coimbatore
India

Abstract- Mobile- ad hoc networks (MANETs) based on cooperative communication (CC) present significant challenges to security issues. The performance of network also to be monitored for the network by achieving high authentication and topology control in MANET has a significant impact on the throughput. In this paper a novel approach has been proposed using Joint authentication and topology control (JATC) scheme to increase the throughput thereby achieving stochastic optimization. This approach presents Channel Bandwidth enhancement to JATC scheme for minimizing information loss. The appropriate usage of channels is to reduce the bandwidth consumption. Utility functions are arrived for appropriate channel bandwidth prompting to match bandwidth and transmission demand. This mechanism ensures operators to express different requirements in terms of throughput and availability.

Keywords- MANET, Cooperative communication, JATC, Channel Bandwidth.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices which is connected by wireless. Each device in a MANET can free to move independently in any of the direction, and will therefore change its links to other devices frequently. Each must have forward traffic unrelated to its own use, and therefore to be a router.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate with them or may be connected to the larger Internet. MANETs are a kind of a wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

Based on asymptotic results on k-connectivity, a simple scheme for the topology control is projected. The scheme is used to generate several topologies under highly mobile environment. Through recreation and investigation we show that this scheme results in higher connectivity even under mobile conditions as the number of nodes increases.

We also show that even though the scheme uses changing transmission power, the overall consumption of power in the network remains comparatively identical, and is less when we use a constant transmission power as the number of nodes increases. In order to use the proposal, the nodes need to his equally distributed. We prove that under cyclic boundary conditions the stationary distribution of nodes, moving according to (a variant of) the random waypoint model, is uniform. We analyze the effective throughput with upper layer authentication schemes and physical-layer schemes related to channel conditions and relay selections for CCs. A joint authentication and topology control (JATC) scheme is proposed to improve the throughput. JATC is described as a discrete stochastic optimization problem, which does not require earlier perfect channel status but only channel approximation.

Bandwidth required transmitting a signal or bandwidth of a transmission media plays an important role in any form of communication (wired or wireless). This paper explains the importance of bandwidth and how we can choose modulation technique, multiple access technique and other parameters for broadband communication so that the available bandwidth gets enhanced. A technique for bandwidth enhancement of a given amplifier is presented. Adding several inter stage passive matching networks enables the control of transfer function and frequency response behavior. Parasitic capacitances of cascaded gain stages are isolated from each other and absorbed into passive networks.

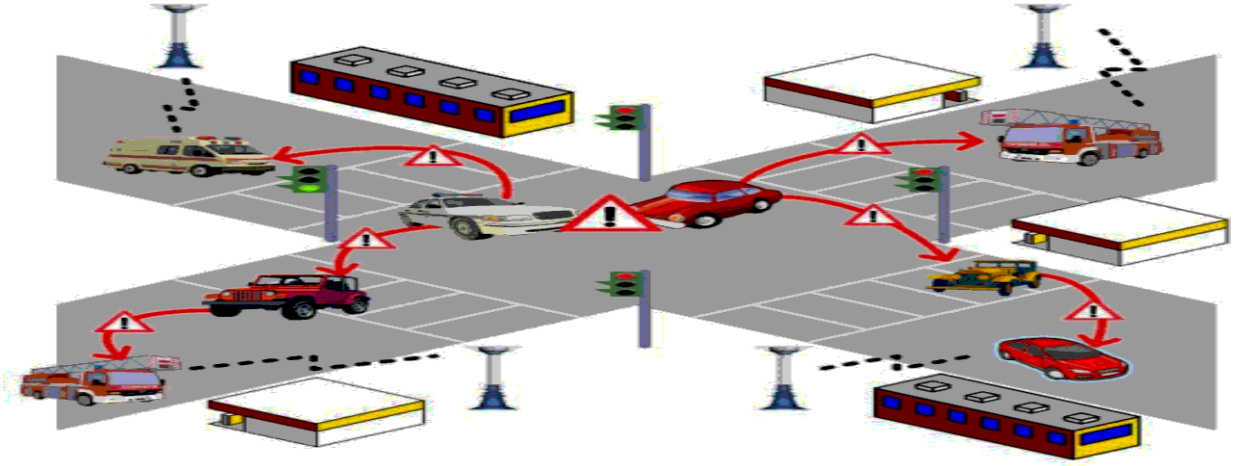

Fig 1:Mobile Ad-hoc Network

II. RELATED WORK

Methods adopted for increasing the energy efficiency of the Wireless networks. The data transmission is successfully carried over in the wireless sensor networks with the cooperative communication technique [1]. But direct transmission is more efficient than cooperative transmission. To overcome this problem, in adaptive transmission, cross layer scheme [1] is provided to increase the energy efficiency of the data transmission. For the MANET security issues Joint Topology Control and Authentication Design is used for the mobile networks [3]. This method improves the throughput and has a better convergence rate. PHY layer [2] increases the utility of resources thereby increasing the capacity of the whole network [6]. An authentication protocol for increasing the throughput of the network.

The expected network capacity is determined by various factors: wireless channel data rate in the physical layer [4] spatial reuse development and intrusion detection in the link layer, topology control traffic steadiness in routing, various traffic methods etc. In the physical layer [4], controlling the data rate of the channels is one of the main aspects to be considered. Theoretically, Shannon capacity model can be used for derivation of the channel bandwidth [7].

TESLA broadcast authentication protocol is used for more transmission and reducing the packet loss during data transmission [5].It is not a signature based mechanism. To overcome the authentication problems and also to enable the receivers to verify the data [7] and ensure that they are not modified, we use this method.

A DT utilizes no relays, whereas an MT does not combine signals at the destination. Therefore, the selection of the transmission manner and the selection of the relay node comprise a wireless link and thus determine the network topology in MANETs. A link refers to a logical connection for two neighboring nodes working possibly in one of the three transmission modes. The best type of transmissions and the best relay node can be determined according to the current channel conditions. In this paper, consider only dual-hop transmissions since dividing a neighboring link into too many hops may introduce more duplicates of packets in the network and thus decrease network capacity.

III. PROPOSED METHOD

A. System Model for Topology Control

In general, a network topology can be described as a Graph $G(V, E)$, including all its nodes V and link connections E among them. Network topology control is essential to determine where to deploy links and how links work to form a *good* topology, which can optimize some global network performance while preserving some global graph property (i.e., connectivity). Since it is difficult to collect the entire network information in MANETs, topology control in such networks should be resolved by distributed schemes, which are executed by each individual node to optimize all the neighboring connections. Usually, a general distributed topology control problem is modeled as

$$G*N = \text{argmax}f(GN) \text{ or } G*N = \text{argmin}f(GN)$$

where $GN(VN, EN)$ relates to the neighboring graph obtained by each node. The objective of topology control is achieved by adjusting some controllable parameters that affect link status, such as transmission power, antenna direction, channel assignment, cooperative level, and transmission manners. Considering that CC may improve communication reliability and efficiency, transmissions in a MANET may be one of the following: direct transmissions (DTs), multi hop transmissions (MTs), and CCs. In CCs, the destination node decodes a combined signal from the source node and the relayed signals of interest from assistant relays. In this paper, a decode-and-forward (DF) scheme is used. The other two types of transmissions can be regarded as special cooperative transmissions.

B. Authentication Protocol

A computationally efficient protocol for e2e and HBH integrity verification and authentication based on hash chains has been proposed .It combines concepts of interactive signatures and Merkle Trees to design a lightweight

mechanism that is adaptive and flexible to the limited resources of mobile devices. A hash chain is a successive application of any cryptographic hash function $H(x)$ by hashing a random seed variable x. It is recursively and sequentially calculated by $hi = H(hi-1)$, where $h1 = H(x)$. Thus, $hi = Hi(x)$ in a hash chain of length i. The hash chain is usually applied in an opposite sequence since hi will not be revealed without $hi-1$. In the authentication protocol, the final constituent of the hash chain, i.e., the *anchor hi*, is initially provided by the owner to the verifier.

The verifier can confirm the authenticity of the owner with $hi-1$ by subsequently hashing $hi-1$. The operation process of the protocol begins with an initial handshake to exchange the anchors of hash chains. As shown in Fig. 1, the protocol consists of a four-way packet exchange for each signed data message *mj* . The signer establishes a signature Merkle Tree before the four-way exchange. Let S1, A1, S2, and A2 denote the packets in the four-way exchange, respectively. In Fig. 1, the S1/A1 packet consists of the root of the signature/ acknowledgment Merkle Tree *r* and a fresh hash-chain element of the signer/verifier.

The signer and verifier maintain their own signature and acknowledgment hash chains to identify themselves. Message *mj* is disclosed in S2, along with a set of complementary branches *{Bc}*. On receiving S2, the verifier obtains messages *mj* and *{Bc}* and uses them to regenerate the Merkle Tree root. Comparing this root with the received *r* in S1, message is authenticated, and its integrity is verified. An index *xi* and a secret *si* are contained in A2 to identify message *mj* . Merkle Tree size the number of signed data blocks parameter for authentication protocol. Overhead has to be less than packet size or payload will drop to zero. Increase of packet size improves authentication strength of a packet due to increased sizes of complementary branches may decrease transmission throughput. Throughput is determined by jointly considering topology control and authentication setting.

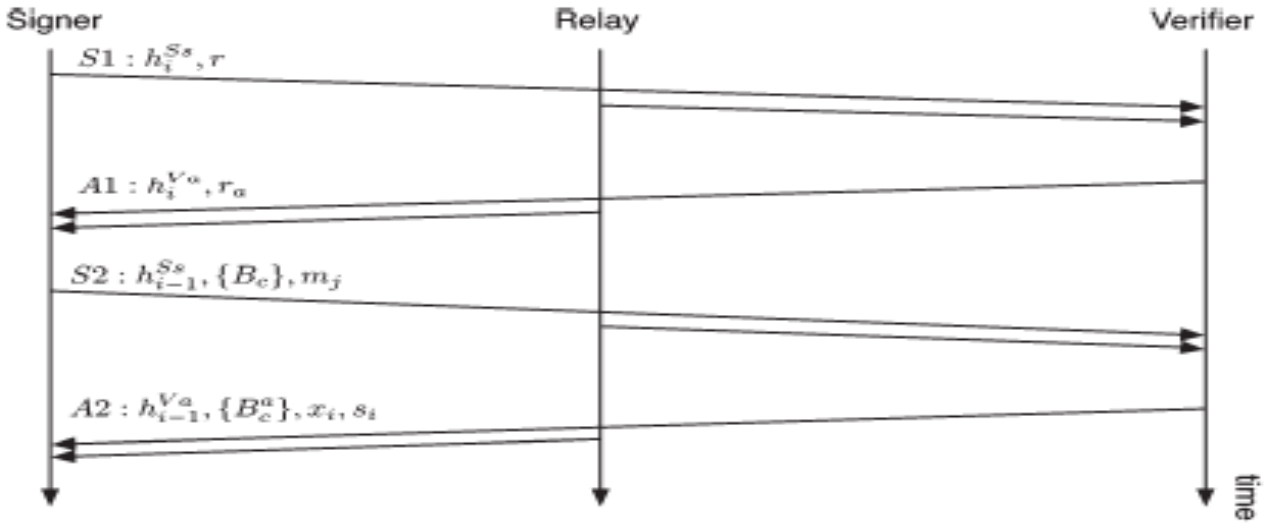

Fig.2. Authentication protocol for cooperative transmissions.

C. Throughput Analysis

The authentication protocol provides throughput adaptation in its configuration. The total amount of payload transmitted with a single pre signature is expressed by

$$spayload = n \cdot (spacket - sh\ (\_log2\ n\_ + 1))$$

where *s*packet is the packet size, *sh* is the hash size, and *n* is the size of the Merkle Tree. A tradeoff between the signed payload of S2 packets in a Merkle Tree and the additional signature data accompanied with S2 packets is essentially measured, as the size of the set *{Bc}* of complementary branches logarithmically grows with the number of data chunks (S2 packets) in Merkle Tree. When this set approaches packet size *s*packet, *s*payload drops to zero. We are interested in the throughput performance of the protocol. To improve its reliability, an ARQ scheme is needed. As selective-repeat (SR)-ARQ has been proven to outperform other forms of ARQ schemes, we use SR-ARQ in the study. Detailed studies of ARQ schemes are beyond this paper. The throughput is defined as the average rate of successfully message delivery over a communication channel.

D. Joint Authentication and Topology Control

The effect of throughput depends on some coupled configuration has three types of transmissions have distinct throughput. Even for MTs and cooperative transmissions are selection of relays has significant impact on throughput each relay has its own PHY-layer parameters. SNR in wireless channel results in smaller outage probability and higher outage capacity of better BER. Relay with best BER for cooperative link is preferred for improve throughput. The packet size managed by segmentation technique has impact on throughput efficiency. Larger packet size increases amount of payload in that packet to increases packet error rate and decreases throughput as well as design on the packet size.

E. Channel Assignment and Topology Control

Joint channel assignment and topology control consists of throughput estimation module and estimates the throughput for specific channel assignment and node connectivity. Estimated consider rate diversity, location of mesh nodes and gateways, channel model, transmission power, and receiver sensitivity. Channel and link selection module captures both path loss and adjacent channel interference. The channel assignment defines node connectivity. An interface's transmission rate depends on the destination interface it communicates with transmission rate. Transmission rate in turn influences the throughput achieved by that link all other links in the same transmission range operate on the same channel. Set of links between nodes contains elements of the form denoting a link between nodes i and j operating on channel k. Exist multiple links between two mesh nodes, operating on different channels. Different nodes communicate with same node on the same channel. K is the number of assigned channels and I is the number of interfaces in node. The channel and topology control objective is to maximize the aggregate utility.

F. Utility Function and Channel Bandwidth

Utility is a function of the throughput of links between nodes i and j. The utility for node pair depends only on total throughput achieved by links between two nodes. Network's aggregate utility is the sum of logarithms, more value is placed on node pairs with small throughput imposes fairness across different node pairs. Addition of weights, which reflect the relative importance of links. Throughput estimation is based on link conflict graph, and maximal cliques. All links belonging to same maximal clique have an equal throughput share. Links belonging to more than one clique are assigned the throughput of the most congested one. Throughput estimation for each clique depends on time for each link belonging to the clique to transmit one packet inversely proportional to its transmission rate. Estimation procedure proceeds by assigning throughputs with increasing throughput values follows a max-min sharing of wireless resources.

IV. CONCLUSION

Since security and throughput are two major concerns of MANETs, we have considered them together in this paper for CC-MANETs. With the analysis under an authentication protocol, we have developed a JATC scheme, which tunes the parameters of up-layer authentication protocol and PHY-layer transmission settings to increase resource utilization and throughput capacity of the network. The proposed Channel Bandwidth Enhancement to JATC used to utilize the functions arrived to appropriate channel bandwidth. Topology control with bandwidth adaptation reduces channel bandwidth usage. Data loss arises due to dynamic topology is minimized and maintain minimal authentication and integration overhead.

REFERENCES

[1] Quansheng Guan, F. Richard Yu, Shengming Jiang, and Victor C. M. Leung, "Joint Topology Control and Authentication Design Ad Hoc Networks with Cooperative Communications" IEEE Transactions on Vehicular Technology, Vol.61, No.6, July 2012.

[2] A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," IEEE Commun. Mag., vol. 42, no. 10, pp. 74–80, Oct. 2004.

[3] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[4] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA broadcast authentication protocol," RSA CryptoBytes, vol. 5, no. 2, pp. 2–13, 2002.

[5] T. Heer, S. Götz, O. G. Morchon, and K. Wehrle, "ALPHA: An adaptive and lightweight protocol for hop-by-hop authentication," in Proc. ACM CoNEXT, Madrid, Spain, 2008, pp. 1–12.

[6] H. Yang, F. Ricciato, S. Lu, and L. Zhang, "Securing a wireless world," Proc. IEEE, vol. 94, no. 2, pp. 442–454, Feb. 2006.

[7] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," SIGMOBILE Mobile Comput. Commun. Rev., vol. 6, no. 3, pp. 106–107, Jul. 2002.

[8] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004.

[9] M. Burkhart, P. von Rickenbach, R.Wattenhofer, and A. Zollinger, "Does topology control reduce interference?" in Proc. 5th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., Tokyo, Japan, May 2004, pp. 9–19.

[10] E. Lloyd, R. Liu, M. Marathe, R. Ramanathan, and S. Ravi, "Algorithmic aspects of topology control problems for ad hoc networks," Mobile Netw. Appl., vol. 10, no. 1/2, pp. 1

