ADVANCEMENTS OF CORMAN TECHNOLOGY IN MULTI-HOP WIRELESS NETWORKS WITH RUMOR RIDING MECHANISM

R GNANAJEYARAMAN*

DEEPUMON.A.S**

Abstract

The link quality variation of wireless channels has been a challenging issue in data communications until recent explicit exploration in utilizing this characteristic. The same broadcast transmission may be perceived significantly differently, and usually independently, by receivers at different geographic locations. Furthermore, even the same stationary receiver may experience drastic link quality fluctuation over time. The combination of link-quality variation with the broadcasting nature of wireless channels has revealed a direction in the research of wireless networking, namely, cooperative communication. Research on cooperative communication started to attract interests in the community at the physical layer but more recently its importance and usability have also been realized at upper layers of the network protocol stack. In this article, we tackle the problem of opportunistic data transfer in mobile ad hoc networks. Our solution is called Cooperative Opportunistic Routing in Mobile Ad hoc Networks (CORMAN). It is a pure network layer scheme that can be built atop off-the-shelf wireless networking equipment. The new implementation part contains the security features ,which provides the accurate node selection and its location access mechanism and also provides the security of data from unauthorized user. Mainly there three new features are added with the CORMAN mechanism. There are 1. Mobile Prediction(MP)-Nodes that frequently change their motion need to frequently update their neighbors, since their locations are changing

* Asso.Prof, Dept. of CSE, SBM College of Engineering & Technology, Dindigul, Tamilnadu

** Final B.E, Dept. of CSE, SBM College of Engineering & Technology, Dindigul, Tamilnadu

dynamically 2.On-Demand Learning(OLD)-The MP rule solely, may not be sufficient for maintaining an accurate local topology. According to this rule, whenever a node overhears a data transmission from a new neighbor, it broadcasts a beacon as a response. 3. Rumor Riding(RR)-It is employing a random walk concept, RR issues key rumors and cipher rumors separately, It provides a high degree of anonymity.

Index Terms- Cooperative communication; opportunistic routing; mobile ad hoc networks; proactive source routing; forwarder list update; On-Demand Learning; Mobility prediction; Rumor Riding

INTRODUCTION

A mobile ad hoc network is a wireless communication network, where nodes that are not within direct transmission range of each other will require other nodes to forward data. It can operate without existing infrastructure, supports mobile users, and falls under the general scope of multi-hop wireless networking. Such a networking paradigm originated from the needs in battlefield communications, emergence operations, search and rescue, and disaster relief operations. Later, it found civilian applications such as community networks. A great deal of research results have been published since its early days in the 1980's [1]. The most salient research challenges in this area include end-to-end data transfer, link access control, security, and providing support for real-time multimedia streaming. The network layer has received the most attention when working on mobile ad hoc networks. As a result, abundant routing protocols in such a network with differing objectives and for various specific needs have been proposed [2]. In fact, the two most important operations at the network layer, i.e., data forwarding and routing, are distinct concepts. Data forwarding regulates how packets are taken from one link and put on another. Routing determines which path a data packet should follow from the source node to the destination. The CORMAN mechanism gives more importance to its broadcasting mechanism and maintenance of path and topology instead of security. So now security is the main challenge in CORMAN. To provide secure features within the CORMAN mechanism there are three new security features are implement here 1.Mobile Prediction(MP)-Nodes that frequently change their motion need to frequently update their neighbors, since their locations are changing dynamically 2.On-Demand Learning(OLD)-The MP rule solely, may not be sufficient for maintaining an accurate local topology. According to this rule, whenever a node overhears a data transmission from a new neighbor, it broadcasts a beacon as a response. 3. Rumor Riding (RR)-It is employing a random walk concept, RR issues key rumors and cipher rumors separately, It provides a high degree of anonymity. The system is going to prepare compare the performance of CORMAN with that of AODV. It selects AODV as the baseline because AODV is a widely adopted routing protocol in MANETs. From the experimental results, it can be observed that CORMAN has a Packet Delivery Ratio of about 95% for dense networks (i.e., $250 \leq l \leq 500$ m). As the node density decreases, this rate gradually goes down to about 60%. In contrast, AODV's PDR ranges between 60% and 80% for dense networks and quickly drops to around 20% for sparse (less dense network) networks.

RELATED WORK

The utilization of the broadcasting nature of wireless channel sat the link layer and above has a relatively recent history compared to the efforts at the physical layer. Proposes an innovative handshake technique, called Selection Diversity Forwarding (SDF), to implement downstream forwarder selection in a multi hop wireless network, where multiple paths are provided by the routing module. In this case, a sender in the network can dynamically choose from a set of usable downstream neighbors that present high transient link quality. For the sender to make the decision, the IEEE 802.11 Distributed Coordination Function (DCF)-based DATA/ACK handshake is enhanced. Such a handshake is the first opportunistic utilization of link quality variation in multi-hop wireless networks at the link and network layers. The coordination in SDF is somewhat expensive and its over head needs to be significantly reduced for it to be more practical. The performance features of the CORMAN with the AODV are follows. From the experimental results, it can be observed that CORMAN has a Packet Delivery Ratio of about 95% for dense networks (i.e., $250 \leq l \leq 500$ m). As the node density decreases, this rate gradually goes down to about 60%. In contrast, AODV's PDR ranges between 60% and 80% for dense networks and quickly drops to around 20% for sparse (less dense network) networks.

This variation occurs by means of link quality. The dense network will have strong link quality whether the sparse network would have weak quality among the nodes. The end-to-end delay and its variance of CORMAN and AODV are now going to be estimated. When the node density is higher (i.e., $250 \leq l \leq 500$ m), CORMAN has a shorter delay than AODV. For sparser scenarios (i.e., $550 \leq l \leq 1000$ m), CORMAN's delay is slightly longer than AODV but comparable. The maximum delay the CORMAN achieved is 0.12(seconds) in the dense networks but the maximum delay of AODV estimated is 0.39≅4.0 (seconds) CORMAN's performance is compared to AODV based on different rates of node velocity and the network dimensions. In addition, higher security is achieving by introducing the new concept called rumor riding which ensures that the data packet can reach to destination with more than 95% accuracy. We adopt the following terms defined in ExOR to describe similar concepts in CORMAN:

• Batch size — number of packets in a batch. It has the same value for all packets in a given batch.

• Forwarder list size — number of forwarders on the forwarder list. It has the same value for all packets in a given batch.

• Packet number — index of the packet in the batch.

• Forwarder number — index of the forwarder on the forwarder list. It indicates which node on the list has just transmitted the data packet.

• Batch map — an array whose size equals the batch size. Each element of the map is indexed by the packet number and its value is the forwarder number of the highest priority forwarder that this packet has reached.

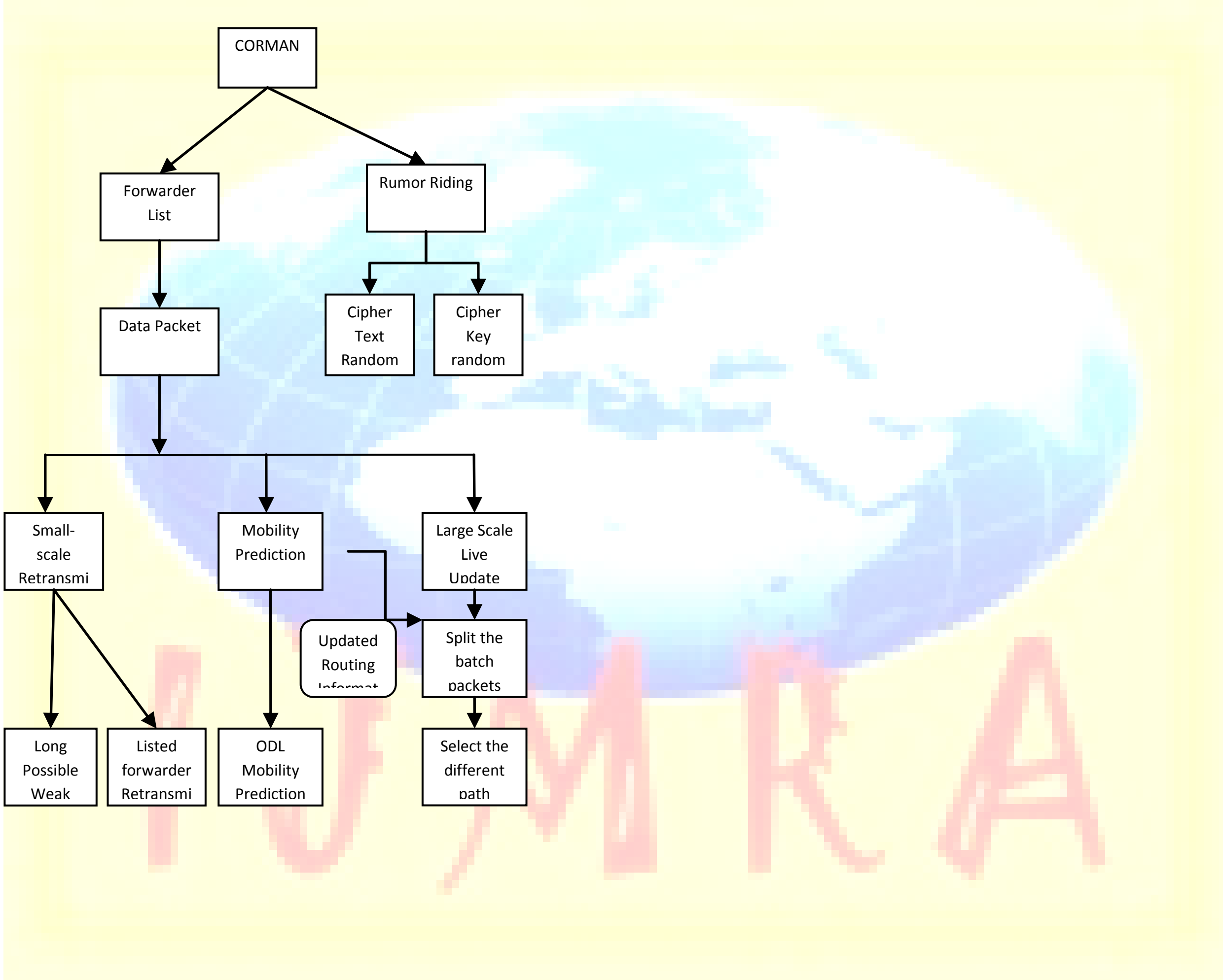
• Fragment — subsets of packets in the current batch which are sent together from a given forwarder.

OVERVIEW OF CORMAN

CORMAN is a network layer solution to the opportunistic data transfer in mobile ad hoc networks. Its node coordination mechanism is largely in line with that of ExOR and it is an extension to ExOR in order to accommodate node mobility. Here, we first highlight our objectives and challenges in order WANG et al.: CORMAN: a novel cooperative opportunistic routing scheme in mobile ad hoc networks to achieve them. Later in this section, we provide a general description of CORMAN. The details of CORMAN will be presented in Sections IV and

V.A. Objectives and challenges CORMAN has two objectives. 1) It broadens the applicability of ExOR to mobile multi-hop wireless networks without relying on external information sources, such as no depositions. 2) It incurs a smaller overhead than ExOR by including shorter forwarder lists in data packets.

SYSYEM ARCHITECTURE:



EXISTING SYSTEM:

In Existing anonymity approaches peers have to pre-construct an anonymous path before transmission. In crowds there is need to establish a anonymous path before transmission. Crowd is an path based protocol .Existing works, for example P5 employ the flooding pattern, which is not suitable for P2p systems due to the huge traffic overhead. The end-to-end delivery, which is used by the path based approaches, however may compromise the anonymity of the initiator or responder but fails due to traffic and weak links. Initiator has to collect large numbers of IP addresses.

MODULES DESCRIPTION:

Analysis of the Local Topology:

A lightweight proactive source routing protocol is used so that each node has complete knowledge of how to route data to all other nodes in the network at anytime. When a flow of data packets are forwarded towards their destination, the route information carried by them can be adjusted by intermediate forwarders.

Routing and protocol Adaptation:

In this phase the forward list is constructed and installed in a data packet, the source node has updated knowledge of the network structure within its proximity but its knowledge about further areas of the network can be obsolete due to node mobility. A short forwarder list carried by data packets implies that they tend to take long and possibly weak links rather than selecting strong neighbor one. For opportunistic data transfer, this could be problematic since the list may not contain enough redundancy in selecting intermediate nodes.

- **Large Scale Live Update**

When a batch of packets are forwarded along the route towards the destination node, if an intermediate node is aware of a new route to the destination, it is able to use this new route to forward the packets that it has already received. There are a few implications of this. First, this new route will also be used to forward the subsequent packets of the same batch.

- **Small-Scale Retransmission:**

To enhance the reliability of packet transmission between two consecutive listed forwarders taken f1 and f2, this project employs the mechanism of small-scale retransmission. First, a node r should be a neighbor of both two listed forwarders f1 and f2. Node r can learn this by looking up its neighbor list. Second, the separation distance between d (f1, f2), should be greater than d(f1, r) and d(r, f2). That is, it must be within the region. The node separation distance can be estimated using the RSSI (Received Signal Strength Indicator) recorded when packets are received.

Analysis position Update:

- **MP rule**

Upon receiving a beacon update from a node each of its neighbors records node current position and velocity and periodically track node location. The goal of the MP rule is to send the next beacon update from node when the error between the predicted location and node's actual location is greater than an acceptable threshold. The priority of a forwarding candidate is decided by its distance to the destination. The nearer it is to the destination, the higher priority it will get. When a node sends or forwards a packet, it selects the next hop forwarder as well as the forwarding candidates among its neighbors. The next hop and the candidate list comprise the forwarder list.

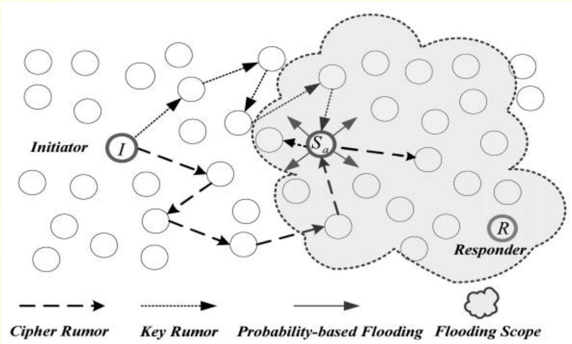
- **ODL Rule**

The MP rule solely, may not be sufficient for maintaining an accurate local topology. In ODL RULE, the average number of new neighbors that enter the radio range of a node between two successive forwarding operations. The node will only become aware of these new neighbors when it forwards the next packet, since these neighbors will broadcast beacons announcing their presence in response to the packet transmission. According to this rule, whenever a node overhears a data transmission from a new neighbor, it broadcasts a beacon as a response. The location updates are piggybacked on the data packets and that all nodes operate in the promiscuous mode.

RUMOR RIDING:

In this module, a non-path-based anonymous P2P protocol is proposed called Rumor Riding (RR). In RR, it first let an initiator encrypt the query message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher texts take random walks separately in the system, where each walk is called a rumor. Once a key rumor and a cipher rumor meet at some peer, the peer is able to recover the original query message and act as an agent to issue the query for the initiator. This agent peer is known as a shower node. . Thus, the rumors serve as the primitives of this protocol to achieve mutual anonymity and meet the design objectives. In RR, anonymous paths are automatically constructed via the rumors' random walks. Neither the initiator nor the responder needs to be concerned with path construction and maintenance.

RR employs a symmetric cryptographic algorithm to achieve anonymity, which significantly reduces the cryptographic overhead for the initiator, the responder, and the middle nodes. In addition, as initiating peers have no requirement on extra information for constructing paths, the risk of information leakage, caused by links that are used for peers to request the IP addresses of anonymous proxies, is eliminated.



We propose Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems. Employing a random walk mechanism, RR takes advantage of lower overhead by mainly using the symmetric cryptographic algorithm. We propose a non-path-based anonymous P2P protocol called Rumor Riding (RR). In RR, we first let an initiator encrypt the query message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher texts take random walks separately in the system, where each walk is called a rumor. Once a key rumor and a cipher rumor meet at some peer, the peer is able to recover the original query message and act as an agent to issue the query for the initiator. We call the agent peer as a shower in this paper. The similar idea is also employed during the query response, confirm, and file delivery processes.

Advantages

- Non-path based approach(Rumor Riding)
- Used AES cryptographic algorithm
- Reduce cryptographic overhead for the Initiator, Responder and Middle nodes

- Improve system performance
- Random chosen Neighbor
- Avoid blind-flooding

1. Rumor Riding

A non-path-based anonymous P2P protocol called Rumor Riding (RR). In RR, we first let an initiator encrypt the query message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher texts take random walks separately in the system, where each walk is called a rumor. Once a key rumor and a cipher rumor meet at some peer, the peer is able to recover the original query message and act as an agent to issue the query for the initiator. We call the agent peer as a shower.

2. Rumor Generation and Recovery

RR employs the AES algorithm to encrypt original messages. The key size is 128-bit. To determine whether a pair of cipher and key rumors hit, we employ a Cyclic Redundancy Check (CRC) function to attach a CRC value, CRC (M), to the message M. For received key rumors and cipher rumors, the shower S uses AES to recover a message M' and the checksum CRC(M'). It then performs the CRC function to the recovered M' and compares the result with CRC (M'). If they match, the shower S is aware that it has successfully recovered a message M.

3. Query Issuance

When an initiator I wishes to issue an anonymous query, it first generates the query content q, and a public key K. Node I then uses an AES cryptographic algorithm to encrypt q into a cipher text C with a symmetric key K. It organizes the key K and the cipher text C into two query rumors, qK and qC. In Gnutella, each packet is labeled with a Descriptor ID, a string that uniquely identifies the packet. RR also uses the descriptors to identify rumors. Thus, two random number strings, IDqK and IDqC, are used to label the two rumors. After generation, I forwards the rumor messages to two randomly chosen neighbors, as illustrated by the dashed and dotted lines in Fig. 1. The query cipher rumor and the query key rumor then start their random walks.

4. Query Response

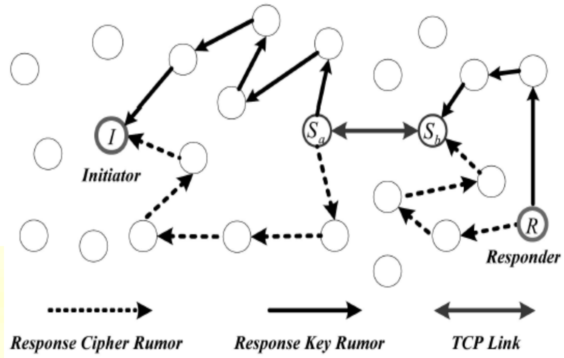


Fig.2

When a receiving node the query has a copy of the desired file, it becomes a responder R. To respond to the query, R encrypts the plain text of the response message r, using the initiator's public key Ki. After being sent out from R, two rumors start their random walks in the system. We illustrate the procedure in Fig. 2. RR guarantees that at least one pair of rumors meet at a certain peer Sb. We use lrK and lrC to denote their paths from R to Sb. Sb decrypts the cipher text in rC with the key in rK, and recovers the IP address of shower Sa

EVALUATION:

The benefits of this project are further confirmed by undertaking evaluations in realistic network scenarios, which account for localization error, realistic radio propagation and sparse network. Both theoretical analysis and simulation results show that it achieves excellent performance even under high node mobility with acceptable

CONCLUSION

In this article, we have proposed CORMAN as an opportunistic routing scheme for mobile ad hoc networks. CORMAN is composed of three components. 1) PSR—a proactive source routing protocol, 2) large-scale live update of forwarder list, and 3) small-scale retransmission of missing packets. All of these explicitly utilize the broadcasting nature of wireless channels and are achieved via efficient cooperation among participating nodes in the network. Essentially, when packets of the same flow are forwarded, they can take different paths to the destination And also the effectiveness of the CORMAN mechanism and the implementation of the new security mechanism in this project there are three modules1. MP rule (mobility prediction) 2.ODL Rule (On demand learning)3. Rumor Riding (RR) Rumor Riding is an lightweight and non-path-based mutual anonymity protocol for P2P systems, Rumor Riding (RR). Using a random walk concept, RR gives key rumors and cipher rumors separately, and expects that they meet in some random peers. Shower is a peer where key rumor and cipher rumor meet and decryption can be done and send to responder. Rumor Riding (RR) provides a high degree of anonymity and outperforms existing approaches in terms of reducing the traffic overhead and processing latency. It eliminates to collect large number of IP addresses when sending a data.

REFERENCES

[1] I. Chlamtac, M. Conti, and J.-N. Liu, “Mobile Ad hoc Networking:Imperatives and Challenges,” Ad Hoc Networks, vol. 1, no. 1, pp. 13– 64, July 2003.

[2] R. Rajaraman, “Topology Control and Routing in Ad hoc Networks: A Survey,” SIGACT News, vol. 33, pp. 60–73, June 2002.

[3] S. Biswas and R. Morris, “ExOR: Opportunistic Multi-Hop Routing for Wireless Networks,” in Proc. ACM Conference of the Special Interest Group on Data Communication (SIGCOMM), Philadelphia, PA, USA, August 2005, pp. 133–144.

[4] P. Larsson, “Selection Diversity Forwarding in a Multihop Packet Radio Network With Fading Channel and Capture,” ACM Mobile Computing and Communications Review, vol. 5, no. 4, pp. 47–54, October 2001.

[5] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, “Trading Structure for Randomness in Wireless Opportunistic Routing,” in Proc. ACM Conference of the Special Interest Group on Data Communication (SIGCOMM), Kyoto, Japan, August 2007, pp. 169–180.

[6] C. Fragouli, J.-Y. L. Boudec, and J. Widmer, “Network Coding: an Instant Primer,” SIGCOMM Computer Communication Review, vol. 36, pp. 63–68, January 2006.

[7] I. Leontiadis and C. Mascolo, “GeOpps: Geographical Opportunistic Routing for Vehicular Networks,” in Proc. IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), Helsinki, Finland, June 2007, pp. 1–6.

[8] S. Yang, F. Zhong, C. K. Yeo, B. S. Lee, and J. Boleng, "Position Based Opportunistic Routing for Robust Data Delivery in MANETs," in Proc. 2009 IEEE Conference on Global Telecommunications (GLOBECOM), Honolulu, Hawaii, USA, December 2009, pp. 1325–1330.

[9] S. Murthy, "Routing in Packet-Switched Networks Using Path-Finding Algorithms," Ph.D. dissertation, University of California - Santa Cruz, 1156 High Street, Santa Cruz, CA 95064, United States, 1996.

[10] J. Behrens and J. J. Garcia-Luna-Aceves, "Distributed, Scalable Routing based on Link-State Vectors," in Proc. ACM SIGCOMM, 1994, pp. 136– 147.

[11] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," Mobile Networks and Applications, vol. 1, no. 2, pp. 183–197, October 1996.

[12] Z. Wang, C. Li, and Y. Chen, "PSR: Proactive Source Routing in Mobile Ad Hoc Networks," in Proc. 2011 IEEE Conference on Global Telecommunications (GLOBECOM), Houston, TX USA, December 2011.

[13] Z. Wang, Y. Chen, and C. Li, "A New Loop-Free Proactive Source Routing Scheme for Opportunistic Data Forwarding in Wireless Networks," IEEE Communications Letters, to appear.

[14] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[15] M. K. Marina and S. R. Das, "Routing Performance in the Presence of Unidirectional Links in Multi hop Wireless Networks," in The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), Lausanne, Switzerland, June 2002, pp. 12–23.