Security and Energy Efficient Communication Scheme in Mobile Ad Hoc Networks

R.Aiyshwariya Devi[1],E.Devi priya[2]

Dept of Informattion Technology PSNA college of Engineering and Technology

Dindigul

aish.sbm@gmail.com

eedevipriya@gmail.com

***Abstract*— In mobile ad hoc networks (MANETs),security has become one of the major issues for data communication and every node overhears every data transmission in the and thus consumes energy unnecessarily. Some MANET routing protocols such as Dynamic Source Routing (DSR) collect route information via overhearing, they would suffer if they are used in combination with 802.11 PSM. we will propose a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks.**

Key words—**Dynamic routing, DSDV, Energy Balance, Energy Efficiency, Power saving mechanism.**

I INTRODUCTION

In mobile ad hoc networks (MANETs) is energy conservation due to the limited lifetime of mobile devices. Since wireless communication could be responsible for more than half of total energy consumption a great deal of effort has been devoted to develop energy-aware network protocols such as Power-aware routing and transmit power control (TPC)-based algorithms Essentially, they have concentrated on reducing energy spent for active communication.

Among many well-known designs for cryptography based systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) [21] are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads[1], [7], [13], especially on gateway/host performance and effective network bandwidth. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) [5] is adopted for encryption/decryption for IPSec [2]. Another alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim. The intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data.

The main goal of this paper is to make the 802.11 PSM applicable in a MANET with Dynamic Source Routing (DSR) [6] and to achieve an additional energy saving by identifying and eliminating unnecessary communication activities. More specifically, this paper has been motivated by the following two observations. First, a main trouble in integrating the DSR protocol with 802.11 PSM comes from unnecessary or unintended overhearing. Overhearing improves the routing efficiency in DSR by eavesdropping other communications to gather route information but it spends a significant amount of energy. Second, it is important to note that most of network layer solutions developed for MANETs including DSR depend on broadcast flood of control packets. Unconditional forwarding of broadcast packets is wasteful and even harmful because it generates many redundant rebroadcasts. This paper proposes a message overhearing and forwarding mechanism, called Random-Cast, which makes a judicious balance between energy and network performance. In Random Cast, a node may decide not to overhear (a unicast message) and not to forward when it receives an advertisement during an ATIM window, thereby reducing the energy cost without deteriorating the network performance. Key contributions of this paper are threefold: 1) It presents the Random Cast protocol that is designed to employ the IEEE 802.11 PSM in multihop MANETs. Unlike previous approaches, where nodes need to switch between AM and PS mode, they consistently operate in the PS mode in Random Cast. This has not been studied elsewhere in the literature to the best of authors' knowledge. 2) In Random Cast, a transmitter can specify

the desired level of overhearing to strike a balance between energy and throughput.

More importantly, it helps avoid the semantic discrepancy found in most of MANET routing protocols. For example, in DSR, when a node transmits a unicast packet, it in fact expects that all of its neighbors overhear it as if it is a broadcast packet. This is not the case in the proposed Random Cast protocol. 3) Compared to our earlier work [19], this paper shows that the problem of unconditional or unnecessary forwarding of broadcast packets can also be taken care of in the Random Cast framework. The performance of the proposed Random Cast scheme is evaluated using the ns-2 network simulator [1] in comparison to 802.11, 802.11 PSM, and On-Demand Power Management (ODPM) [32]. ODPM is one of the most energy-efficient MAC schemes developed for MANETs and is discussed in detail in Section 2.2. According to the simulation results, the proposed algorithm reduces the energy consumption as much as 50 percent and 31 percent compared to the original IEEE 802.11 PSM and ODPM, respectively. On the other hand, network performance such as its packet delivery ratio (PDR) could be at a disadvantage with Random Cast because nodes are not able to transmit or receive packets when they are in sleep state.

In order to examine the performance trade-offs, we measure a combined metric, called energy good put (Kbytes/Joule), which is defined as the number of bytes delivered per unit energy. Random Cast achieves as much as 64 percent and 63 percent higher energy good put than 802.11 PSM and ODPM, respectively, which exhibits the overall benefit of Random Cast.

The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets. The proposed algorithm should be easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol (RIP) for wired networks [16] and Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks [20], over existing infrastructures. These protocols shall not increase the number of control messages if the proposed algorithm is adopted.

The rest of the paper is structured as follows: Section 2 presents the background information on the DSR routing protocol and IEEE 802.11 PSM.Section 3 explains the Security Enhanced Dynamic Routing, Section 4 presents the proposed Random Cast protocol and its integration with DSR.Section 5 is devoted to Extensive performance analysis. Section 6 draws conclusions and presents future directions of this study.

II BACKGROUND

The objective of this work is to explore a Security and Energy efficient communication scheme in Mobile Adhoc Networks . It also discusses the effect of overhearing in DSR and argues that unconditional overhearing and rebroadcast is the main reason behind energy inefficiency. It explains 802.11 PSM and previous research work on its use in single-hop and multihop networks. The objective of this work is to explore a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. In general, routing protocols over networks could be classified roughly into two kinds: distance-vector algorithms and link-state algorithms [11]. Distance-vector algorithms rely on the exchanging of distance information among neighboring nodes for the seeking of routing paths. Examples of distance-vector-based routing algorithms include RIP and DSDV.

2.1 DSR Routing Protocol

When a node has a data packet to send but does not know the routing path to the destination, it initiates the route discovery procedure by broadcasting a control packet, called route request (RREQ). When an RREQ reaches the destination, it prepares another control packet, called route reply (RREP), and replies back to the source with the complete route information. Upon receiving an RREP, the source saves the route information in its local memory, called route cache, for later uses. Since nodes move randomly in aMANET, link errors occur and a route information that includes a broken link becomes obsolete. When a node detects a link error during its data transmission, it sends another control packet, called route error (RERR), to the source and deletes the stale route from its route cache. Overhearing improves the network performance by allowing nodes to collect more route information. Nodes in the vicinity of a transmitter would learn about the path to the destination via overhearing.

III SECURITY-ENHANCED DYNAMIC ROUTING

The objective of this section is to propose a distance-vector based algorithm for dynamic routing to improve the security of data transmission. We propose to rely on existing distance information exchanged among neighboring nodes (referred to as routers as well in this paper) for the seeking of routing paths. In many distance-vector-based implementations, e.g., those based on RIP, each node Ni maintains a routing table . in which each entry is associated with **a tuple ðt;WNi ;t;NexthopÞ, where t, WNi;t,** and Next hop denote some unique destination node, an estimated minimal cost to send a

packet to t, and the next node along the minimal-cost path to the destination node, respectively. With the objective of this work in the randomization of routing paths, the routing table shown in Table 1a is extended to accommodate our security-enhanced dynamic routing algorithm.

The proposed algorithm achieves considerably small path similarity for packet deliveries between a source node and the corresponding destination node. However, the total space requirement would increase to store some extra routing information. The size of a routing table depends on the topology and the node number of a network under discussions. In the worst case, we have a fully connected network. For each entry in the routing table shown in Table 1b, the

TABLE 1

An Example of the Routing Table for the Node Ni

Destination Node (t)	Cost $(W_{N_i,t})$	Nexthop
N_1	7	N_6
N_2	8	N_{21}
N_3	9	N_9
⋮	⋮	⋮

(a)

Destination Node (t)	Cost $(W_{N_i,t})$	Nexthop Candidates $(C_t^{N_i})$	History Record for Packet Deliveries to the Destination Node t $(H_t^{N_i})$
N_1	7	$\{\hat{N}_6, N_{20}, N_{21}\}$	$\{(N_2,N_{21}),(N_3,N_6),\cdots,(N_{31},N_{20})\}$
N_2	8	$\{N_9, \hat{N}_{21}\}$	$\{(N_1,N_9),(N_3,N_9),\cdots,(N_{31},N_{21})\}$
N_3	9	$\{\hat{N}_9\}$	$\{(N_1,N_9),(N_2,N_9),\cdots,(N_{31},N_9)\}$
⋮	⋮	⋮	⋮

(b)

additional spaces required for recording the set of node candidates (as shown in the third column of Table 1b) and for recording the routing history (as shown in the fourth column of Table 1b) are OðjNjÞ. Because there are jNj destination nodes at most in each routing table, the additionally required spaces for the entire routing table for one node are OðjNj2Þ.Since the provided distributed dynamic routing algorithm (DDRA) is a distance-vector-based routing protocol for intradomain systems, the number of nodes is limited, and the network topology is hardly fully connected. Hence, the increase of the total space requirement is considerably small. However, the impact of the space requirement on the search time will be analyzed in the following section.

3.1 A Distributed Dynamic Routing Algorithm

The DDRA proposed in this paper consists of two parts:
1) a randomization process for packet deliveries and
2) maintenance of the extended routing table.

3.2.1 Randomization Process

Consider the delivery of a packet with the destination t at a node Ni. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries shown in Procedure 1 is adopted. In this process, the previous next hop hs (defined in HNi t of Table 1b) for the source node s is identified in the first step of the process (line 1). Then, the process randomly pick up a neighboring node in CNi t excluding hs as the next hop for the current packet transmission. The exclusion of hs for the next hop selection avoids transmitting wo consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

Procedure RANDOMIZEDSELECTOR (s,t,pkt)

1: Let hs be the used nexthop for the previous packet delivery for the source node s.
2: if hs 2 CNi t then
3: if jCNi t j > 1 then
4: Randomly choose a node x from fCNi t _ hsg as a nexthop, and send the packet pkt to the node x.
5: hs x, and update the routing table of Ni.
6: else
7: Send the packet pkt to hs.
8: end if
9: else
10: Randomly choose a node y from CNi t as a next hop, and send the packet pkt to the node y.
11: hs y, and update the routing table of Ni.
12: end if

The number of entries in the history record for packet deliveries to destination nodes is jNj in the worst case. In order to efficiently look up the history record for a destination node, we maintain the history record for each node in a hash table. Before the current packet is sent to its destination node, we must randomly pick up a neighboring node excluding the used node for the previous packet. Once a neighboring node is selected, by the hash table, we need Oð1Þ to determine whether the selected neighboring node for the current packet is the same as the one used by the previous packet. Therefore, the time complexity of searching a proper neighboring node is O(1).

IV RANDOMIZED OVERHEARING AND FORWARDING USING RANDOMCAST

This section describes the proposed Random Cast protocol. It is designed to improve energy performance by controlling the level of overhearing and forwarding without a significant impact on network performance. Compared to the algorithms presented in Section 2.2, the proposed scheme assumes that mobile nodes employ 802.11 PSM and consistently operate in the PS mode.

When a node (its MAC address MA) wakes up at the beginning of a beacon interval, it receives an ATIM frame for a unicast packet. The ATIM frame contains the receiver address (DA) and subtype (ID). The node decides whether or not to receive/overhear the advertised packet in the following data transmission period based on DA and ID. It would remain awaken to receive it if one of the following conditions is satisfied:

1. The node is the intended destination (DA ¼ MA).
2. The node is not the destination but the sender wants unconditional overhearing (DA 6¼ MA but ID ¼ 10012).
3. The node is not the destination, but the sender wants randomized overhearing, and the node randomly decides to overhear the packet (DA 6¼ MA, ID ¼ 11012, and decides to overhear).

DSR employs three control packets: RREQ, RREP, and RERR. RREQ is a broadcast, and RREP, RERR, and data are unicast packets. For each of the unicast packets, DSR uses the following overhearing mechanism: Randomized overhearing for RREP packets: An RREP includes the discovered route and is sent from the destination to the originator of the corresponding RREQ packet.

Randomized overhearing for data packets: In DSR, every data packet includes the entire route from source to destination

Unconditional overhearing for RERR packets: When a link (e.g., link B _ C in Fig. 3c) is detected broken, an upstream node (e.g., node B in Fig. 3c) transmits an RERR to the source.

It is better for nodes in the vicinity to overhear this message unconditionally because the stale route information must be propagated as soon and wide as possible.

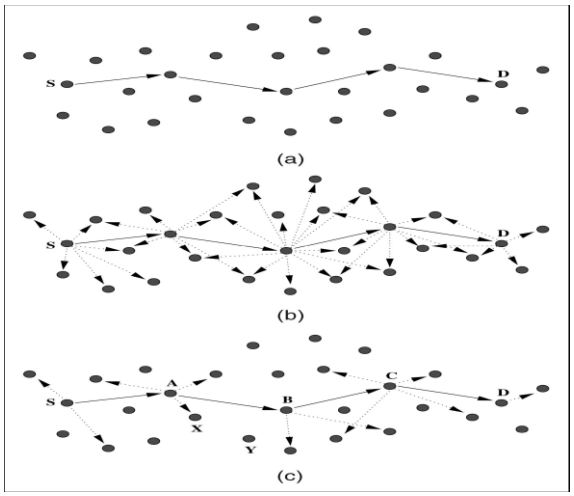

Fig. 1. Delivery of a unicast message with different overhearing mechanisms. (a) no overhearing, (b) unconditional overhearing, and (c) randomized overhearing.

4.1 Random Cast for Broadcast Packets

In Random Cast, when a node sends an ATIM for a broadcast packet, all of its neighbors receive the packet in the following data transmission period but probabilistically rebroadcast it.

. Randomized rebroadcast for RREQ packets: DSR requests a randomized rebroadcast of an RREQ packet to the MAC and the MAC forwards it probabilistically based on PF . If the node is the source of the RREQ, it will ask the MAC to broadcast it unconditionally.
. Unconditional rebroadcast for ARP (address resolution protocol) request packets: ARP request packets are typically single-hop communication. Since the destination node is expected to exist in the transmitter's vicinity, unconditional rebroadcast must be requested to the MAC.

4.2 Random Cast Probability

Basically, each node maintains an overhearing (rebroadcast) probability, PR (PF), determined using the factors Sender ID , Number of neighbors, Mobility, Remaining Battery Energy.

RandomCast at a node (MAC address MA, overhearing probability P_R and rebroadcast probability P_F)

```
/* When it receives a frame */
Upon receiving an ATIM frame (receiver MAC address DA, subtype ID)
    if (DA == BROADCAST) continue to wake up and receive;
    else { /* unicast */
        if (DA == MA) /* the node is the intended destination */
            continue to wake up and receive;
        else if (ID == 1001) /* unconditional overhearing */
            continue to wake up and overhear;
        else if (ID == 1101) { /* randomized overhearing */
            if (rand(0, 1) ≤ P_R)
                continue to wake up and overhear;
            else switch to sleep;
        }
        else switch to sleep;
    }

/* When packet queue is not empty */
Upon being ready to transmit a frame (receiver MAC address DA,
overhearing/rebroadacst level OL requested by DSR/ARP)
    if (DA == BROADCAST) {
        if (OL == unconditional) send an ATIM;
        else if (OL == randomized) {
            if (rand(0, 1) ≤ P_F) send an ATIM;
        }
    }
    else { /* unicast */
        switch (OL) {
            case unconditional: ID = 1001;
            case randomized: ID = 1101;
            case no: ID = 1110;
        }
        send an ATIM with subtype ID;
    }
```

Fig. 2. The Random Cast algorithm.

V PERFORMANCE EVALUATION

The performance of Random Cast is evaluated using ns-2 [1], which simulates node mobility, a realistic physical layer, radio network interfaces, and the DCF protocol. Since ns-2does not support.. The purpose of this section is to evaluate the performance of the proposed algorithm, referred to as the DDRA. A random graph is a graph with a fixed set of vertices, and a link between any two nodes occurs with a given probability. In our experiments, the numbers of nodes in the random topologies are 40, 50, and 60. The link probabilities are 0.1, 0.2, 0.3, and 0.4.

We compare the performance of DDRA with the popular Shortest-Path Routing Algorithm (SPRA) and the Equal-Cost Routing Algorithm (ECRA) used in RIP. In SPRA, only one path with the minimal cost is derived for each source destination pair. On the other hand, more than one path can be accommodated in ECRA if their delivery costs are the same as that of the minimal-cost path. We compare four different schemes: 802.11, 802.11 PSM, ODPM, and Random Cast. 802.11 is unmodified IEEE 802.11 without PSM. As discussed in Section 2.2, ODPM [32] is one of the most competitive energy-efficient schemes developed for multihop networks. For ODPM, a node remains in AM for 5 seconds if it receives an RREP (RREP time-out). It remains in AM for 2 seconds if it receives a data packet or it is a source or a destination node (Data time-out).

Random Cast uses no/unconditional/randomized overhearing depending on the packet type as explained in Section 3. We additionally evaluate RCAST, which employs randomized overhearing like Random Cast but not randomized rebroadcast. This is introduced to see the additional performance enhancement due to randomized rebroadcast.

5.1 Performance Metrics

Performance metrics we have used in our experiments are energy consumption, energy good put, packet delivery ratio (PDR), and packet delay. Energy consumption is measured at the radio layer during the simulation based on the specification of IEEE 802.11-compliant Wave LAN-II [14] from Lucent. The power consumption varies from 0.013 Watt in a low-power sleep state to 0.83, 1.0, and 1.4 Watt in idle listening, receiving, and transmitting states, respectively, [10]. The instantaneous power is multiplied by the time duration to obtain energy consumption. In order to examine the performance trade-offs, a combined metric, called energy good put (Kbytes/Joule), has been used in this paper. It measures the number of bytes delivered successfully per unit energy.

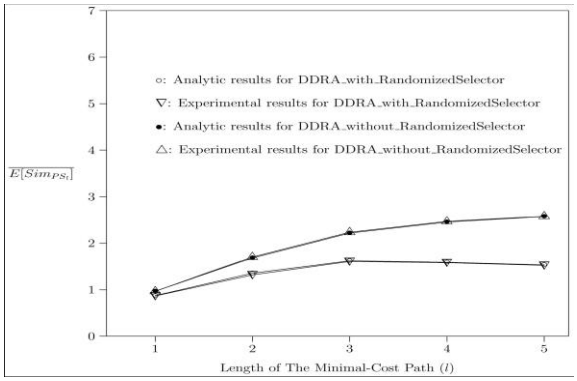

Fig 3. Analytic and experimental results of E½SimPSl _ for AT&T US topology.

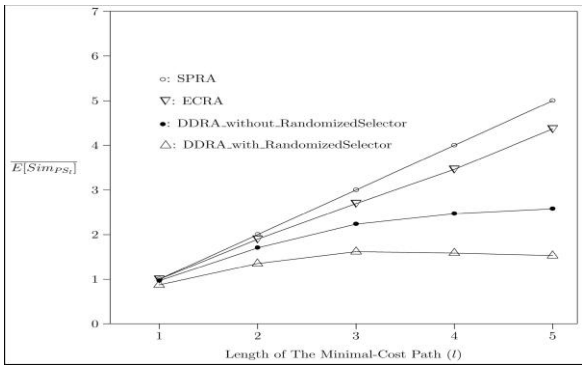

Fig 4 E½SimPSl _ for AT&T US topology

The simulated traffic is constant bit rate (CBR) over User Datagram Protocol (UDP). The interval time of CBR is 10msand the packet size is 1,000 bytes. The simulation time is set to 100 seconds. In addition to path similarity, the performance of the proposed algorithm will be further investigated in terms of average single-trip time (i.e., end to- end delay) and interpacket jitter (the definition of jitter will be described in the following section) caused by the

varying delays resulting from our multipath packet deliveries. In order to investigate the effect of traffic load on throughput for our proposed DDRA, the traffic is also generated based on variable-bit-rate applications such as file transfers over Transmission Control Protocol (TCP). The average packet size is 1,000 bytes, and source-destination pairs are chosen randomly with uniform probabilities.

5.2 Simulation Results

Random Cast achieves a higher PDR, particularly when packet rate is high . This is because of the lower network traffic due to broadcast packets with Random Cast. In addition, it achieves lower energy consumption. Overall, its energy good put is as much as 23 percent better than RCAST.
First, energy consumption due to transmission and sleep is negligible. Second, energy consumption due to idle is in general the largest. Therefore, to save energy, nodes should switch to a sleep state as much as possible while maintaining a good network performance. Third, it is noted that Random Cast exhibits a relatively consistent idle energy regardless the traffic. Fourth, energy consumption due to reception/overhearing
(Rx) increases with traffic.

In short, Random Cast performs on par with other schemes in terms of PDR but achieves a significant energy saving as well as a better energy balance in comparison to
existing schemes. The benefit of Random Cast is significant when traffic is light. This is because nodes stay in low-power sleep state more intelligently in Random Cast.

5.3 Effect of Traffic Load on Throughput

This section elaborates on the effect of traffic load on throughput for SPRA, ECRA, and our DDRA. Note that since the performance of DDRA with Randomized Selector and without Randomized Selector is similar in this case, the curve for DDRA without Randomized Selector will not be plotted.

VI Conclusions

It provides an efficient solution based on Random Cast. The key observation is that unconditional overhearing, which is taken for granted without PSM, is not freely available with PSM. In Random Cast, when a packet is transmitted, nodes in the proximity should decide whether or not to overhear it considering the trade-offs between energy efficiency and routing efficiency. and a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. An analytic study was developed for the proposed algorithm and was verified against the experimental results. A series of simulation experiments were conducted to show the capability of the proposed algorithm, for which we have very encouraging results. We must point out that the proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures.

REFERENCES

[1] Sunho Lim, Chansu Yu, Chita R. Das, " Random Cast: An Energy-Efficient
Communication Scheme for Mobile Ad Hoc Networks", IEEE Network,2009.

[2] Chin-Fu Kuo, Ai-Chun Pang, Sheng-Kun Chan, "Dynamic Routing with Security Considerations", IEEE Network,2009.

[3] S. Agarwal, S.V. Krishnamurthy, R.H. Katz, and S.K. Dao,"Distributed Power Control in Ad-Hoc Wireless Networks," Proc.IEEE Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC'01), pp. 59-66, 2001.

[4] I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," Proc. IEEE Global Telecommunications Conf. (GLOBECOM), 2003.

[5]J.-H. Chang and L. Tassiulas, "Energy Conserving Routing in
Wireless Ad-Hoc Networks," Proc. IEEE INFOCOM, pp. 22-31,
2000.

[6]M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law
Relationships of the Internet Topology," Proc. ACM SIGCOMM'99,
pp. 251-262, 1999.