ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 7, July 2013

Reliable Data Transfer on Dynamic Nodes using Packed Hiding Methods in Ad Hoc Networks

A.Umamaheswaran[1], S.Gopikrishnan[2], R.Saranya[3]

PG Student, Dept. of Computer Science & Engineering, Paavai College of Engineering, Namakkal, Tamilnadu, India [1]

Asst Prof, Dept. of Computer Science & Engineering, Karpagam Institute of Technology, Coimbatore, Tamilnadu, India [2]

Student, Dept. of Computer Science & Engineering, Karpagam Institute of Technology, Coimbatore, Tamilnadu, India [3]

Abstract: This paper addresses the problem of delivering data packets for highly dynamic mobile ad hoc networks in a reliable and timely manner. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. Driven by this issue, we propose an efficient Position-based Opportunistic Routing (POR) protocol which takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. When a data packet is sent out, some of the neighbour nodes that have overheard the transmission will serve as forwarding candidates, and take turn to forward the packet if it is not relayed by the specific best forwarder within a certain period of time. By utilizing such in-the-air backup, communication is maintained without being interrupted. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work, we address the problem of selective jamming attacks in wireless networks.

Keywords: Reliable Data Transfer Packed Hiding Method, Ad hoc Networks, and Selective Jamming Attacks, Geographic Routing

I. Introduction

Mobile ad hoc networks (MANETs) have gained a great deal of attention because of its significant advantages brought about by multi hop, infrastructure-less transmission. However, due to the error prone wireless channel and the dynamic network topology, reliable data delivery in MANETs, especially in challenged environments with high mobility remains an issue. Traditional topology-based MANET routing protocols (e.g., DSDV, AODV, DSR) are quite susceptible to node mobility. One of the main reasons is due to the predetermination of an end-to-end route before data transmission. Owing to the constantly and even fast changing network topology, it is very difficult to maintain a deterministic route. The discovery and recovery procedures are also time and energy consuming. Once the path breaks, data packets will get lost or be delayed for a long time until the reconstruction of the route, causing transmission interruption.

To launch selective jamming attacks, the adversary must be capable of implementing a “classify-then-jam” strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly [34]. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver [34]. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers. The main contributions of this paper can be summarized as follows:

We propose a position-based opportunistic routing mechanism which can be deployed without complex modification to MAC protocol and achieve multiple reception without losing the benefit of collision avoidance provided by 802.11.

In the case of communication hole, we propose a Virtual Destination-based Void Handling (VDVH) scheme in which the advantages of greedy forwarding (e.g., large progress per hop) and opportunistic routing can still be achieved while handling communication voids.

We investigate the feasibility of real-time packet classification for launching selective jamming attacks, under an internal threat model. We show that such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes.

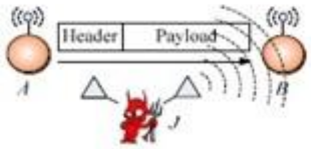

Fig 1 Realization of a selective jamming attack

II. PROBLEM STATEMENT AND ASSUMPTIONS

A. Problem Statement

Consider the scenario depicted in Fig. 1a. Nodes A and B communicate via a wireless link. Within the communication range of both A and B, there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics.

B. System and Adversary Model

- Network Model

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using presaged pair wise keys or asymmetric cryptography.

- Communication Model

Packets are transmitted at a rate of R bauds. Each PHY layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries α/β q data bits, where = is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is α/β qR bps. Spread-spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect wireless transmissions from jamming. SS provides immunity to interference to some extent (typically 20 to 30 dB gain), but a powerful jammer is still capable of jamming data packets of his choosing.

Transmitted packets have the generic format depicted in Fig. 1. The preamble is used for synchronizing the sampling process at the receiver. The PHY-layer header contains information regarding the length of the frame, and the transmission rate. The MAC header determines the MAC protocol version, the source and destination addresses, sequence numbers plus some additional fields. The MAC header is followed by the frame body that typically contains an ARP packet or an IP datagram. Finally, the MAC frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be appended for synchronizing the sender and receiver. 2.2.3 Adversary Model

The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Solving well-known hard cryptographic problems is assumed to be time consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space.

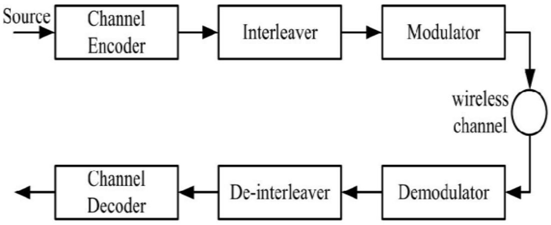

Fig.2.A Generic Communication System Diagram

The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad hoc, mesh, cognitive radio, and wireless sensor networks (WSNs), where network devices may operate unattended, thus being susceptible to physical compromise.

III.POSITION-BASED OPPORTUNISTIC ROUTING

The design of POR is based on geographic routing and opportunistic forwarding. The nodes are assumed to be aware of their own location and the positions of their direct neighbours. Neighbourhood location information can be exchanged using one-hop beacon or piggyback in the data packet's header. While for the position of the destination, we assume that a location registration and lookup service which maps node addresses to locations is available just as in. It could be realized using many kinds of location service. In our scenario, some efficient and reliable way is also available. For example, the location of the destination could be transmitted by low bit rate but long range radios, which can be implemented as periodic beacon, as well as by replies when requested by the source.

When a source node wants to transmit a packet, it gets the location of the destination first and then attaches it to the packet header. Due to the destination node's movement, the multihop path may diverge from the true location of the final destination and a packet would be dropped even if it has already been delivered into the neighbourhood of the destination. To deal with such issue, additional check for the destination node is introduced. At each hop, the node that forwards the packet will check its neighbour list to see whether the destination is within its transmission range. If yes, the packet will be directly forwarded to the destination, similar to the destination location prediction. By performing such identification check before greedy forwarding based on location information, the effect of the path divergence can be very much alleviated.

In conventional opportunistic forwarding, to have a packet received by multiple candidates, either IP broadcast or an integration of routing and MAC protocol is adopted. The former is susceptible to MAC collision because of the lack of collision avoidance support for broadcast packet in current 802.11, while the latter requires complex coordination and is not easy to be implemented. In POR, we use similar scheme as the MAC multicast mode. The packet is transmitted as unicast (the best forwarder which makes the largest positive progress toward the destination is set as the next hop) in IP layer and multiple receptions are achieved using MAC interception. The use of RTS/CTS/DATA/ACK significantly reduces the collision and all the nodes within the transmission range of the sender can eavesdrop on the packet successfully with higher probability due to medium reservation.

Every node maintains a forwarding table for the packets of each flow (identified as source-destination pair) that it has sent or forwarded. Before calculating a new forwarder list, it looks up the forwarding table; an example is illustrated in Table 1, to check if a valid item for that destination is still available. The forwarding table is constructed during data packet transmissions and its maintenance is much easier than a routing table. It can be seen as a trade-off between efficiency and scalability.

The packets in the interface queue taking node A as the next hop will be given a second chance to reroute. For the packet pulled back from the MAC layer, it will not be rerouted as long as node S overhears node B's forwarding.

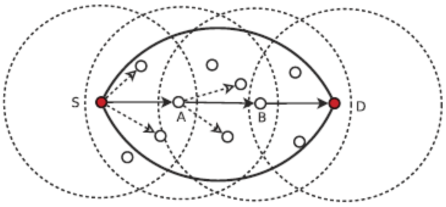

Fig 3 Duplicate Relaying

A. MAC Modification and Complementary Techniques

- MAC Interception

We leverage on the broadcast nature of 802.11 MAC: all nodes within the coverage of the sender would receive the signal. However, its RTS/CTS/DATA/ACK mechanism is only designed for unicast. It simply sends out data for all broadcast packets with CSMA. Therefore, packet loss due to collisions would dominate the performance of multicast-like routing protocols. Here, we did some alteration on the packet transmission scenario. In the network layer, we just send the packet via unicast, to the best node which is elected by greedy forwarding as the next hop. In this way, we make full utilization of the collision avoidance supported by 802.11 MAC. While on the receiver side, we do some modification of the MAC-layer address filter: even when the data packet's next hop is not the receiver, it is also delivered to the upper layer but with some hint set in the packet header indicating that this packet is overheard. It is then further processed by POR. Hence, the benefit of both broadcast and unicast (MAC support) can be achieved.

- MAC Call back

When the MAC layer fails to forward a packet, the function implemented in POR mac call back will be executed. The item in the forwarding table corresponding to that destination will be deleted and the next hop node in the neighbour list will also be removed. If the transmission of the same packet by a forwarding candidate is overheard, then the packet will be dropped without reforwarding again; otherwise, it will be given a second chance to reroute. The packets with the same next hop in the interface queue which is located between the routing layer and MAC layer will also be pulled back for rerouting. As the location information of the neighbours is updated periodically, some items might become obsolete very quickly especially for nodes with high mobility. This scheme introduces a timely update which enables more packets to be delivered. The first question is at which node should packet forwarding switch from greedy mode to void handling mode.

IV. VIRTUAL DESTINATION-BASED VOID HANDLING

In order to enhance the robustness of POR in the network where nodes are not uniformly distributed and large holes may exist, a complementary void handling mechanism based on virtual destination is proposed.

A. Trigger Node

The first question is at which node should packet forwarding switch from greedy mode to void handling mode. In many existing geographic routing protocols, the mode change happens at the void node, e.g., Node B in F. Then, Path 1 (A-B-E-$_{3\ 3\ 3}$) and/or Path 2 (A-B-C-F- $_{3\ 3\ 3}$) (in some cases, only Path 1 is available if Node C is outside Node B's transmission range) can be used to route around the communication hole. From Fig. 3, it is obvious that Path 3 (A-C-F-$_{3\ 3\ 3}$) is better than Path 2. If the mode switch is done at Node A, Path 3 will be tried instead of Path 2 while Path 1 still gets the chance to be used. A message called void warning, which is actually the data packet returned from Node B to Node A with some flag set in the packet header, is introduced to trigger the void handling mode. As soon as the void warning is received, Node A (referred to as trigger node) will switch the packet delivery from greedy mode to void handling mode and rechoose better next hops to forward the packet. Of course, if the void node happens to be the source node, packet forwarding mode will be set as void handling at that node without other choice (i.e., in this case, the source node is the trigger node).

V. IMPACT OF SELECTIVE JAMMING

In this section, we illustrate the impact of selective jamming attacks on the network performance. We used OPNET Modeller to implement selective jamming attacks in two multi hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

A. Selective Jamming at the Transport Layer

In the first set of experiments, we set up a file transfer of a 3 MB file between two users A and B connected via a multi hop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/CTS mechanism was enabled. The transmission rate was set to 11 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were considered:

1. Selective jamming of cumulative TCP-ACKs.
2. Selective jamming of RTS/CTS messages.
3. Selective jamming of data packets.
4. Random jamming of any packet.

In each of the strategies, a fraction p of the targeted packets is jammed. In Fig. 3a, we show the average delay E½Dfor completing the file transfer, as a function of the jamming probability p (averaged over repeated experiments). In Fig. 3b, we show the average throughput E½Tas a function of p. It can be observed that all jamming attacks have significant impact on E½D which grows several orders of magnitude larger compared to the delay in the absence of a jammer. Similarly, the effective throughput drops drastically under both random and selective jamming attacks. TCP performance under jamming of TCP-ACKs can be interpreted by the congestion control mechanism of the TCP protocol. When cumulative ACKs are lost (in our case jammed), the sender has to retransmit all unacknowledged data packets, thus increasing the incurred delay while reducing the effective throughput. At the same time, the sender interprets the loss of ACKs as congestion and throttles its packet transmission rate by reducing the size of the transmission window. This leads to a further slowdown of the application. Note that, for values of $p > 0:4$, the TCP connection is aborted for the case of random and TCP-ACK jamming, due to the repeated time-outs at the sender. depicts the number of packets that were jammed by the adversary for each value of p. Finally, Fig. 3d shows the fraction of time that the jammer remained active. Here, for selective jamming attacks, we assumed that 13 percent of the packet has to be corrupted in order to be dropped. In the case of random jamming, the adversary is not aware of the type of packets transmitted (by means of processing the header of these packets). Hence, he is assumed to jam the entire packet in order to drop it. We observe that selective jamming requires the jamming of approximately one order of magnitude fewer packets than random jamming. This is because, as the packet transmission rate of the sender drops, fewer packets need to be selectively targeted. Moreover, in selective jamming, the fraction of time the adversary remains active is several orders of magnitude less compared to random jamming. From Fig. 3d, we observe that targeting control packets such as RTS/CTS messages and TCP-ACKs yields the lowest jamming activity, because control packets are significantly smaller compared to data packets.

B. Selective Jamming at the Network Layer

In this scenario, we simulated a multi hop wireless network of 35 nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths [19]. Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam non over lapping areas of the network. Three types of jamming strategies were considered: 1) a continuous jammer, 2) a random jammer blocking only a fraction p of the transmitted packets, and 3) a selective jammer targeting route-request (RREQ) packets. In we show the number of connections established, normalized over the number of connections in the absence of the jammers. Fig. 3f shows the fraction of time that the jammer was active during our simulation, for each jamming strategy. We observe that a selective jamming attack against RREQ messages is equally effective to a constant jamming attack. However, selective jamming is several orders of magnitude more efficient as it is illustrated.

VI. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics. We analysed the security of our schemes and quantified their computational and communication overhead.

REFERENCES

[1] Bu-sung lee, chai kiat Yeo, shengbo “Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks” (January 2012) ieee paper puplic Unversity of Singapore YangBookmark:http://do

[2] Mauve. M, Widmer. J, and Hartenstein. H,“A survey on position-based routing in mobile ad hoc networks”, IEEE Netw. , vol. 15, no. 6, pp. 30–39, Nov. 2001.

[3] Heissenbttittel. M, Braun. T, Bernoulli. T, and Wälchli. M, “BLR: Beacon- less routing algorithm for mobile ad-hoc networks”, Comput. Commun. J., vol. 27, no. 11, pp. 1076–1086, Jul. 2004.

[4] Ftissler. H, Widmer. J, Käsemann. M, Mauve. M, and Hartenstein. H, ‘Contention-based forwarding for mobile ad-hoc networks”, Ad Hoc Netw. J., vol. 1, no. 4, pp. 351–369, Nov. 2003.

[5] Zorzi. M and Rao. R.R, “Geographic random forwarding (GeRaF) for ad hoc and sensor networks: Multihop performance”, IEEE Trans. Mobile Comput., vol. 2, no. 4, pp. 337–348, Oct.–Dec. 2003.

[6] Blum. B.M, He. T, Son. S, and Stankovic. J.A, “IGF: A robust state-free communication protocol for sensor networks”, CS Dept., Univ. Virginia, Charlottesville, Tech. Rep. CS-2003-11, 2003.

[7] Chen. D, Deng. J, and Varshney. P.K, “A state-free data delivery protocol for wireless sensor networks”, in Proc. IEEE WCNC, New Orleans, LA, Mar. 2005, pp. 1818–1823.

[8] Ferrara. D, Galluccio. L, Leonardi. A, Morabito. G, and Palazzo. S, “MACRO: An integrated MAC/Routing protocol for geographic forwarding in wireless sensor networks”, in Proc. IEEE Infocom, Miami, FL, Mar. 2005, pp. 1770–1781.

[9] Fang. Q, Gao. J, and Guibas. L.J, ”Locating and bypassing routing holes in sensor networks”, in Proc. IEEE Infocom, Hong Kong, Mar. 2004, pp. 2458–2468.

[10] Karp. B and Kung. H.T, “Greedy perimeter stateless routing for wireless networks”, in Proc. ACM MobiCom, Boston, MA, Aug. 2000, pp.243–254.

[11] Law. Y.W, Palaniswami. M, Hoesel. L.V, Doumen. J, Hartel. P, and Havinga. P, “Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols,” ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38, 2009

[12] Lazos. L, Liu. S, and Krunz. M, “Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks,” Proc. Second ACM Conf. Wireless Network Security, pp. 169-180,2009.

[13] Lin. G and Noubir. G, “On Link Layer Denial of Service in Data Wireless LANs,” Wireless Comm. and Mobile Computing, vol. 5, no. 3, pp. 273-284, May 2004.

[14] Liu. X, Noubir. G, and Sundaram. R, “Spread: Foiling Smart Jammers Using Multi-Layer Agility,” Proc. IEEE INFOCOM, pp. 2536-2540, 2007.

[15] He. T, Stankovic. J.A, Lu. C, and Abdelzaher. T, “SPEED: A stateless protocol for real-time communication in sensor networks,” in Proc. Int. Conf. Distrib. Comput. Syst., Providence, RI, May 2003, pp. 46–55.