ISSN : 2231-0711
IJCSET | April 2011 | Vol 1, Issue 3,140-145

Receiver Anonymity for Unicast Frames by using IEEE 802.11-Compliant MAC Protocol

Pooja Sharma
B.S. Anangpuria Institute of Technology and Management. Faridabad, India

Dr. Deepak Tyagi
St. Anne Marry Education Society, New Delhi

Vibhu Nagpal
B.S. Anangpuria Institute of Technology and Management. Faridabad, India

Abstract- **Mix based systems used for real-time bidirectional traffic actually does very limited mixing, and hence are vulnerable to powerful adversaries. In this paper, we explore the design of a MIX-net based anonymity system in mobile ad hoc networks. The objective is to hide the source-destination relationship in end to end transmission. We survey existing MIX route determination algorithms that do not account for dynamic network topology changes, which may result in high packet loss rate and large packet latency. We then introduce adaptive algorithms to over-come this problem. We also focus on the notion of providing anonymity support at MAC layer in wireless networks, which employs the broadcast property of wireless transmission. We design an IEEE 802.11-compliant MAC protocol that provides receiver anonymity for unicast frames and offers better reliability than pure broadcast protocol.**

1. INTRODUCTION

The IEEE 802.11 protocol is a network access technology for providing connectivity between wireless stations and wired networking infrastructures.

1.1 802.11 MAC Frame

The 802.11 MAC frame, as shown in the figure1, consists of a MAC header, the frame body, and a frame check sequence (FCS). Each frame consists of the following basic components:

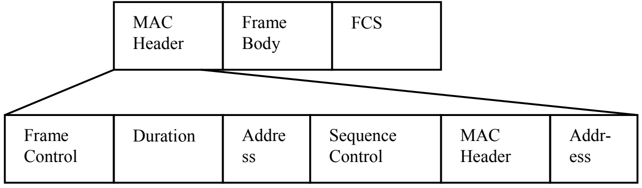

Fig. 1General format of MAC frame in 802.11 standard

a) MAC Header: A MAC header, which comprises frame control, duration, address, and sequence control information;
b) Frame Body: A variable length frame body, which contains information specific to the frame type; c) A Frame Check Sequence (FCS): The Frame Check Sequence (FCS) is the last four bytes in the standard 802.11 frame, often referred to as the Cyclic Redundancy Check (CRC). As frames are about to be sent, the FCS is calculated and appended. When a station receives a frame, it can calculate the FCS of the frame and compare it to the one received. If they match, it is assumed that the frame was not distorted during transmission. d) Frame Control Field: The Frame Control Field, contains control information used for defining the type of 802.11 MAC frame and providing information necessary for the following fields to understand how to process the MAC frame. e) Duration/ID Field: This field is used for all control type frames, except with the subtype of Power Save (PS) Poll, to indicate the remaining duration needed to receive the next frame transmission. f) Sequence Control: The Sequence Control field contains two subfields, the Fragment Number field and the Sequence Number field, as shown in the following figure 2.

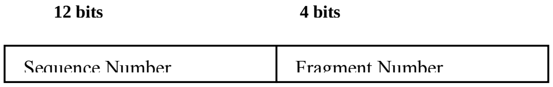

Fig2. Sequence Control

Sequence Number indicates the sequence number of each frame. The sequence number is the same for each frame sent for a fragmented frame
Fragment Number indicates the number of each frame sent of a fragmented frame. The initial value is set to 0 and then incremented by one for each subsequent frame sent of the fragmented frame.
In addition to data frame, which carries application data, the protocol uses a number of control frames (i.e., RTS, CTS, ACK) during the operation. The frame type is specified in the frame control field. Depending on the type, the fields Address 2, Address 3, Sequence Control, Address 4 and Frame Body may be omitted. In any data frame, there must be addresses of source and destination node of the frame. If the destination address is all-1's, then it is a broadcast frame; otherwise, it is a unicast frame.

1.2 Wired Equivalent Privacy (WEP) Protocol

The 802.11 standard defines a Wired Equivalent Privacy (WEP) protocol for encrypting the contents of a data frame,. WEP encryption uses the RC4 [1]symmetric stream cipher with 40-bit and 104-bit encryption keys. WEP provides data confidentiality services by encrypting the data sent between wireless nodes. Setting a WEP flag in the MAC header of the 802.11 frame indicates that the frame is encrypted with WEP encryption. WEP provides data integrity by including an integrity check value (ICV) in the encrypted portion of the wireless frame. WEP defines two shared keys:

- Multicast/global key. The *multicast/global key* is an encryption key that protects multicast and broadcast traffic from a wireless AP to all of its connected wireless clients.
- Unicast session key. The *unicast session key* is an encryption key that protects unicast traffic between a wireless client and a wireless AP and multicast and broadcast traffic sent by the wireless client to the wireless AP. WEP relies on a secret key k shared between the communicating parties, i.e., sender and intended receiver of the frame.

Although serious flaws were found in current implementations of WEP protocol, which may lead to successful attacks against content privacy of encrypted messages, all these flaws can be fixed with improved key management, increased key length, or even new and stronger cryptographic algorithm. So, for the purpose of this paper, we assume that an eavesdropper does not have the capability of performing effective cryptanalysis to break the cipher. In a wireless network, if there is no congestion in a network or any other interference from the adversary then every node which is within the transmission range of the sender will receive the frame. If this feature is combined with frame encryption, which we can be employed to hide the receiver of a unicast frame. The explanation of this feature is as follows:

1. The sender makes a frame which consists on MAC header and the frame body and inserts a pseudo header between them. The pseudo header which is inserted by the sender consists the address of the intended receiver of the frame and other control fields. The pseudo header and the old frame body form a new frame body, which is passed to the RC4 cipher for WEP encryption.
2. For making this new frame as an unsuspicious broadcast frame the sender sets the destination address in the MAC header to all-1's, and transmits it on the radio link.
3. All the nodes that are lying within the connection range of sender tries to decrypt the frame payload.

Although this scheme is easy to implement and provides cheap receiver anonymity, but it consists of serious reliability problem. In IEEE 802.11 protocol, unicast frames and broadcast frames are treated differently. As we know, the wireless network often suffers loss due to collision and interference. In a transmission connection range when the recipient node receives a unicast frame, the recipient node is required to send an ACK frame to the sender node in order to send the acknowledgement that it receives the frame. If the sender node does not receive the expected ACK from the receipt ant node within a specified time period , it assumes that the transmission is failed and will retransmit the frame (up to a maximum number) after a random "backoff delay". With stop-and-wait ARQ [2], the MAC protocol can achieve a very high success rate with unicast frame transmission. On the other hand, broadcast frames are transmitted with a much lower reliability in 802.11 because recipient node of a broadcast frame need not to send ACK frame to the sender node that it receives the frame and also the sender node need not to retransmit a broadcast frame even if it is corrupted or lost during the transmission. Apparently, if no extra measures are taken, the anonymous frames , which are unicast frames originally but converted into broadcast frames, will suffer the low reliability as well. There are various solutions available in order to solve this problem. An effective one is that a receiver send an anonymous ACK frame to the sender when it receives the successfully. There is a possibility of traffic analysis attack by an eavesdropper in this approach because ACK frame is timing link with previous data frame. Another approach is to use existing reliable broadcast schemes. In literature, there are several MAC protocols which were proposed by researchers to improve reliability of broadcast transmission in IEEE 802.11 networks [10, 4, 8, 3, 5, 6]. However, a reliable broadcast scheme has different goal from an anonymous transmission scheme. In a broadcast scheme the intention of the sender is that all the intended recipient receive the transmitted frame successfully. For achieving this objective , the sender retransmitted the data frames many times until from all the intended receiver it receives the ACK frame or the sender gives up. If we use this scheme to provide anonymity, the utilization of the system could be low, because a lot of retransmissions are unnecessary. However**,** we propose a new approach to reliable anonymous transmission of unicast frames. This approach is based on batching and polling techniques. We can achieve the maximum amount of reliability by retransmitting only the lost frames. So it requires the receiver of an anonymous data frame to acknowledge receipt. However, instead of the receiver node sending an ACK frame actively, the source node sends POLLs to a set of neighbor nodes and receives REPLY's from each of them. The set of polled nodes serves as an anonymity set for the receiver node.

2. A RELIABLE ANONYMOUS TRANSMISSION SCHEME FOR UNICAST FRAMES

This approach is based on batching technique and polling technique. Batching technique is used to implement anonymous data transmission and polling technique to implement anonymous acknowledgment.

2.1 Preliminary

The 802.11 family uses a MAC layer known as CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) for basic channel access. Carrier Sensing Range (*Rcs*) determines the range within which a transmitter triggers carrier sense detection. This is usually determined by the antenna sensitivity. In IEEE 802.11 MAC, a transmitter only starts a transmission when it senses the media free. When a sender node wants to transmits a frame, first of all the signal is propagated from the transmitter to a receiver. During the propagation , the signal suffers from the attenuation and also loses considerable power. When a signal arrives, whether a receiver can decode it and receive the transmitted frame correctly or not depends on two conditions:

1. The receiving signal power is above the Rx Threshold;
2. The signal-to-noise ratio (SNR) is above the Capture Threshold.

The Rx Threshold decides the transmission range R_{tx}, within which a frame can be successfully received by the intended recipient if there is no interference from other radios. The transmission range is mainly determined by transmission power and radio propagation properties (i.e., attenuation).

The Capture Threshold decides the interference range. R_i, which is the maximum distance between the receiver and an effective interfering node. In addition, R_i is a function of distance between transmitter and receiver, d, as well. Both R_{tx} and R_i are determined by transmitting power, antenna gains, and signal attenuation model. According to [7], when signal attenuation follows the two-way ground model, the following relationship exists:

$Ri = 1.78d$

From the above equation, if the value of d is lager it depicts a higher probability that a transmission experiences interference from other nodes. When d is larger than $R_{cs}/2.78 = 0.36 \times R_{cs}$ (198 meters in our simulation), there might exist nodes within the interference range of the receiver, but beyond the carrier sensing range of the sender. These nodes are called hidden nodes. Nodes within the interference range of a receiver are usually called hidden nodes. When the receiver is receiving a packet, if a hidden node also tries to start a transmission concurrently, collisions will happen at the receiver. When a signal is propagated from a transmitter to a receiver, whether the signal is valid at the receiver largely depends on the receiving power at the receiver.

When a hidden node is transmitting, the sender cannot detect it and the result is that the sender starts its own transmission, but the transmission will fail because the hidden node's transmission interferes with it and the collision will occur.. This problem is illustrated in Figure 3, where node C is a hidden node to node A. In this example, transmission from C to D can go through and is not interfered by A's transmission.

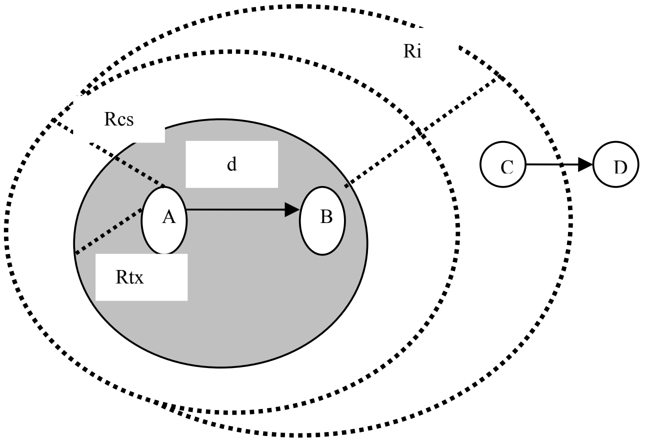

Fig.3 Hidden Node Problem

2.2. **Anonymous MAC Protocol Description**

Each unicast frame is converted into an encrypted broadcast frame in order to hide the recipient from the eavesdropper. The procedure of conversion is already described above, with receiver address being saved in the pseudo-header and being hidden. The sender inserts a pseudo header between the MAC header and the frame body. The pseudo header consists the address of the intended receiver of the frame and other control fields. The pseudo header and the old frame body form a new frame body, which is passed to the RC4 cipher for WEP encryption. All transmissions appear as broadcast frames, to an outside eavesdropper. Each node makes the collection of data frames and form their batches and then transmits them. The formed batches are forwarded to different nodes that are lying within the transmission range, i.e. neighbors. Before sending the frames on the transmission channel first of all the sender checks the availability of particular neighbors by means of polling. To increase the probability of successful transmission, the sender uses a polling mechanism to check the availability of each receiver before transmitting data. During the polling process, the sender sends POLL frames to each neighbour individually and expects to receive REPLY frames from each of them. If a polled node successfully receives the poll and replies, then it means that there is no interference at the node and the node is available for receiving data frames. If a polled node does not reply, then it means that the node did not receive the POLL frame, probably due to interference or due to the congestion, and thus, is not available for receiving data frames thereafter. There is a small interval of time between the Polls and replies. On the basis of replies receiving from the neighbors or receivers, the sender constructs a batch of data frames and sends all the batches. To increase the probability of successful reception, data frames addressed to neighbors that reply polls have higher priority of being selected into the batch.

The POLL/REPLY frames which are created by the sender have another functionality, i.e., acknowledgement. The sender assigned a sequence number to the each frame. In a POLL, the sender asked about receiving status of transmitted frames to check whether the frame has been received by the intended receiver or lost during the transmission. In a REPLY, the polled node reports the sequence numbers of received frames. The sender only retransmits lost frames (up to a maximum number of retransmissions). The format of a POLL frame constructed by the sender is shown in Figure 4 .Duration is the time period which is required to complete the current poll. It is the combination of transmission time of a REPLY frame plus one SIFS interval, SIFS - Short Inter Frame Space, is used to separate transmissions belonging to a single dialog (e.g. Fragment-Ack), and is the minimum Inter Frame Space. RA specifies the node address that is being polled , TA is the address of the node transmitting the POLL frame, , Sequence is used by the ARQ protocol, and Padding is a number of random bytes. The last three fields in a POLL frame are encrypted.

Frame Control	Duration	RA	TA	IV	Sequence	Padding	FCS

Fig. 4. POLL frame format

The format of a REPLY frame is shown in Figure 5 , where RA is the address of the node transmitting POLL, Sequence and Bitmap are used by the ARQ protocol, and Padding is a number of random bytes. The last four fields in a REPLY frame are encrypted.

Frame Control	Duration	RA	IV	Sequence	Bitmap	Padding	FCS

Ciphertext

Fig. 5. REPLY frame format

Pseudo Header

MAC Header	IV	RA	Sequence	Padding	Message	FCS

Ciphertext

Fig. 6. Anonymous data frame

Figure 6. shows the format of an anonymous data frame, where RA is the address of the intended recipient node, Sequence is the identification number of the frame, and Padding is a number of random bytes. The three fields above comprise the pseudo header which contains the receipt ant address.

A. Sender's Protocol

For the purpose of maintaining the list of frames that are waiting to be transmitted or retransmitted, each node maintains a FIFO queue. When a new frame is entered in a list from the upper layer, the new frame assigned a sequence number. The sender and receiver use this sequence number in order to find out the lost frames and retransmit the lost frames. For the purpose of finding the lost frame, each node i.e. p maintains a variable SN_{pq} (Sequence Number) with respect to each neighbor node q. We initialized SN_{pq} to 0 at the system setup time. When a new frame comes to node q, then node p assigns the current value of SN_{pq} to the new frame and increments SN_{pq} by 1. This ensures that node q receives frames from node p with contiguous sequence numbers without any disturbance. If a number is missing, then it indicated that the frame has been lost during transmission. Each node p in the network maintains a sending window [LSN_{pq} , HSN_{pq}]with respect to each neighbor node q . The [LSN_{pq} , HSN_{pq}] is maintained to record the range of sequence numbers of frames stored in the queue. LSN_{pq} is the lowest sequence number of frames, from p to q, currently in the queue, while HSN_{pq} is the highest sequence number. Node p updates LSN_{pq} in two conditions:

a) The Node q sends the acknowledgement of receiving of the frame with sequence number LSN_{pq} to the node p.

b) There is a restriction for the node p , that node p will not transmit the frame with sequence number LSNpq after a maximum number of attempts (4 in our simulations) and finally discards it. For the purpose of recording the number of transmission send by the node p ,the node p maintains a "retry counter" for each frame in the queue.

If the queue is not empty then at each node p , the following algorithm is executed:

1. The node p executes the carrier sense multiple access with collision avoidance (CSMA/CA). For a mobile node to transmit, it shall sense the medium to determine if another mobile node is transmitting. If the medium is not determined to be busy for greater than or equal to a DIFS (DCF IFS) period, the transmission may proceed.
2. By analyzing all the receivers of the frame which are present in the queue., the node p makes a polling set. If the size of the polling set is smaller than a preset minimum value (referred to as MIN _POLLING_ SET_ SIZE), nodes in p's neighbor set are randomly selected to add in.
3. Node p polls each node which are contain in the polling set at a random order. The steps for polling are taken by the node p as follows:
   a) Node p sends a POLL frame to the first node in the polling sent and wait for the listen. If the polled node is q, then the sequence field in the POLL frame carries the current value of LSN_{pq} . If the node p find out that the channel is still free after two SIFS intervals, then the node p polls the next node. Otherwise, the polled node transmits the REPLY frame to the node p. If the node p is convinced by the REPLY frame received from the polled node , node p will update its state based on information in it (e.g., releasing acknowledged frames, advancing the sending window, incrementing retry counters of unacknowledged frames), and sends the POLL frame for the next node after one SIF S interval. In case , if the node p receives a corrupted REPLY frame due to the congestion or interference, or if during the SIFS interval , the transmission channel is busy , node p will abort the current transmission and go to step 1 after backing off a random number of slot times.
   b) If a node fails to reply consecutive polling for a maximum number of times (7 in our simulations), the link is assumed to be broken and all the remaining frames that stays in the queue , sent by the sender on that link are wash out from the sender's queue. The retry limit for polling is set higher than that for retransmitting data. This prevents unnecessary loss of data when the receiver is just experiencing transient interference.
4. There is only one possibility where node p reaches towards the step 4 i.e. where all nodes in the polling set have been polled and node p either receives a convincing REPLY frame or it gets nothing from each node. The nodes which send REPLY frames successfully are called "available receivers". If the queue of available receivers is empty, then node p will abort the current transmission and go to step 1 after backing off a random number of slot times; otherwise, node p selects a set of data frames referred to as batch from its sending buffer to transmit. The batch size is controlled by two system parameters: MIN _BATCH _SIZE and MAX_ BATCH_ SIZE. When node p creates the batch of data frames , it should choose frames addressed to available receivers first. If all such frames have been chosen and the batch size is still less than MIN_ BATCH_ SIZE, then node p can choose frames addressed to other receivers. In our experiments, MIN_BATCH_SIZE and MAX _BATCH _SIZE take values of 1 and 4 respectively. During transmission, the frames in a batch are transmitted consecutively with a time spacing equal to SIFS.

B. Receiver's Protocol

The node q maintains a receiving window is maintained which is used to record the sequence number of the received frames. In Selective Repeat ARQ protocol, two variables are used to implement a receiving window: a Lowest Bound LB_{qp} and a one-byte Bitmap BM_{qp}. From the node p all the data frames whose sequence number is lower than LB_{qp} have been received. However, the BM_{qp} highlights those data frames whose sequence numbers is higher than LB_{qp}. If we are considering the n-th bit of BM_{qp} is 1, it indicates the frame which has been received having a sequence number LB_{qp}+n.. For example, a LB_{qp} of 100 and a BM_{qp} of 11100110 indicate that node q has correctly received frames 0-99, 101, 102, 105, 106, 107, whereas frames 100, 103, 104 were lost. Node q updates its receiving window in two cases:

a) When q received a POLL from the node p , if LSN_{pq} > LB_{qp}, it means that the sender node p has updates its sending window and given up its attempts to retransmit frames lower than LSN_{pq} . This is due to reason when node q suffering from temporary severe interference and failed to reply node p's polling for a certain number of times. In this case, node q synchronizes its receiving window with node p's sending window by advancing LB_{qp} to LSN_{pq} .

b) If the sequence number of the REPLY frame received from the node p matches with LB_{qp}, then node q can updates its receiving window, i.e., incrementing the LB_{qp} by 1 and then right-shifts the BM_{qp} by one bit. Node q repeat the whole adjustment until the lowest bit of BM_{qp} is 0. If the sequence number of the REPLY frame received from the node p is larger than LB_{qp} and is not a duplicate, the BM_{qp} is updated to indicate the receiving status.

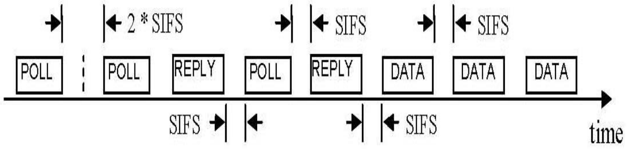

Fig. 7. An illustration of the scheme

Unlike many Selective Repeat ARQ based protocols, in our scheme , we do not maintain a "receiver buffer" at the MAC layer in order to hold-of-sequence frames . Instead, a receiver passes each received frame immediately to the upper layer (i.e., network). There are two reasons. First, this reduces the queuing delay. Second, frames transmitted on a link belong to different end-to-end flows and typically have different next hop receivers. Frame loss due to the interference or due to the congestion of one flow should not influence the frame delivery of other flows. Therefore, we can enhance the overall network performance or the throughput by relaxing the in-sequence constraint . The protocol has been shown in Figure 7. In the figure, the first polled node does not send a REPLY frame to the sender, probably not receiving the POLL. Therefore, after waiting for the REPLY frame ,the sender sends the second POLL (to a different node) after two SIFS intervals. Since if the channel is free for DIFS, any node can send the REPLY frame to the sender . Therefore without waiting for the transmission time of a REPLY frame, the sender transmitting the second POLL earlier, thus it prevents any neighbor from interrupting the polling process.

The second and third POLLs are replied. The sender node received the REPLY frame which is transmit immediately after one SIFS interval by the each polled node. Data frames in the current batch are transmitted continuously, with one SIFS spacing between two consecutive frames. In the whole process the medium never remains idle for more than 2 × SIFS.

3. PROBABILITY OF TRACING THE SOURCE AND DESTINATION

We try to find out the traceability of a source and destination connection in presence of compromised nodes. The traceability pc (c depicts as connection) is defined as the probability that an adversary becomes aware of the source and destination of the connection. So in case, if the source or the destination o a connection is a compromised node, then its traceability is 1. Therefore, in the following, we believe that both sender and the destination of the connection are trustworthy.

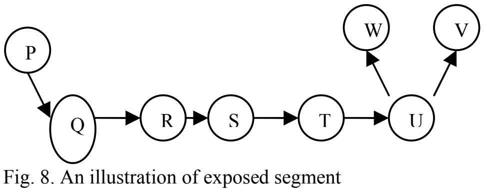

Fig. 8. An illustration of exposed segment

In an end to end connection node Q received the packet from the node P as shown in figure 8 and forward to node R which in turn forward the packet to the node S. Suppose node S is the compromised by the attacker when it received the packet from its corresponding node R. The node S also has the responsibility to forward the packet to node T. The adversary trace out that node Q, R, S, T, U are the consecutives nodes and called this path as exposed segment. If the neighbouring node of S i.e. R and T are compromised then the exposed segment has been extended to R's or T's neighbour and so on. The main objective of an adversary is to find out the connection from which the data packet belongs to and to trace out how many nodes exists on the exposed segment. Taking an example where there are N no. of connections and each connection has n (i = 1, 2, · · · ,N) paths sharing the segment. Then the probability that the packet belongs to the ith connection is

$$\frac{n_i}{\sum_{j=1,2,.....N} nj}$$

We take an assumption that each connection c has a path set $p^{(c)}$ and the different paths in the connection are used to deliver packets in a round-robin fashion. Obviously each path contains the different consecutives nodes i.e. different exposed segments, therefore the chances of the packet for being compromised is different on each path . When a packet take a path which contains K non-adjacent exposed segments, the adversary has K chances to make a correct guess about which connection the packet is associated with.

Table1. Numerical Results for Connection Traceability

Compromised nodes (%)	traceability
0.05	0.08
0.1	0.2
0.15	0.27
0.2	0.38
0.25	0.44
0.3	0.53
0.35	0.59
0.4	0.67
0.45	0.72
0.5	0.78

The probability of successful detection is where p_i is the adversary's successful-detection probability at the *i*-th segment. The traceability of the connection is the average detection probability over all

$$1-\prod_{i=1}^{N}(1-p_i)$$

connection paths, since each path has the same chance of being taken. In order to derive the numerical result we create a network of 50 nodes and establish the network connection between all the nodes to make them as pair. For each connection, we find the shortest path set. We choose the compromised nodes from the network, for tracing out the percentage of compromised nodes. Table 1 gives the average traceability over all connections as the percentage of compromised nodes varies. It is shown that when having less than 10% of compromised nodes, the connection traceability is less than 20%. When 50% nodes are compromised, most of the connections could be traced.

Here we present simulation results on the performance of the proposed scheme. We simulated the scheme using the ns-2 simulator [9] and carried out simulations in a 50-node static network. We randomly distribute the nodes in a 1000m x

1000m square area. There are 20 CBR connections in the network where source and destination of each connection being randomly picked. The source node of each connection which wants to send the data packet to these respective destinations generates packets of fixed size, namely 512 bytes. We vary the average data generation rate to produce different traffic loads. We show the data packet delivery fractions under different traffic loads in Figure 9. For the purpose of effective comparison, we also show the performance of "pure" broadcast scheme, i.e., without getting the feedback form the destination whether it received the data packet or not. We observe that pure broadcast is not effective because the pure broadcast does not provide the confirmation of transmitting all the data frames successfully, even the in the case where the traffic is low and when traffic load increases, its delivery fraction drops fast.

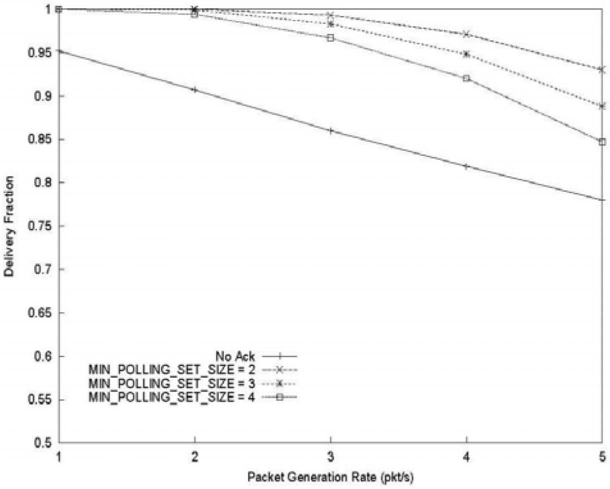

Fig. 9. Data packet delivery ratio

At the same time, our scheme achieves significantly higher delivery fractions. The figure also illustrates the effects of the minimal polling set size on the performance. When a larger polling set is required, the duration of the polling process has to be longer, which increases the probability that a data frame is corrupted by hidden nodes' transmissions.

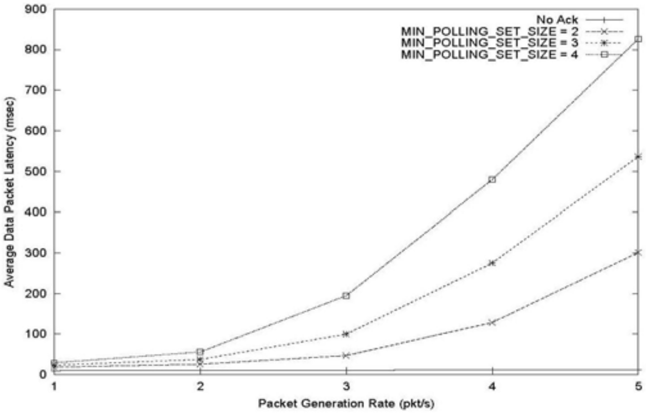

Fig. 10 End-to-end data packet latency

Figure 10, shows the average source and destination data packet latency under different traffic loads. As we consider the static network , therefore there is no delay in transmitting the data packet. We also ignore the CPU processing delay at each intermediate node. Therefore, the end-to-end packet latency includes queuing delays, retransmission delays and propagation delays. Our scheme on an average has much higher packet latency than unreliable, pure broadcast scheme due to the retransmission and batching. When the minimal polling set size increases, the packet latency increases very fast, especially when the traffic load of transmitting the packet is high . The reason is there is a higher probability of the data retransmission failure when the polling set is larger, which makes each node wait for a longer time before next retry.

4. CONCLUSION

In this paper, we explore the design of a MIX-net based anonymity system in mobile ad hoc networks. The objective is to hide the source-destination relationship in end to end transmission. We survey existing MIX route determination algorithms that do not account for dynamic network topology changes, which may result in high packet loss rate and large packet latency. We then introduced adaptive algorithms to over-come this problem. We also focussed on the notion of providing anonymity support at MAC layer in wireless networks, which employs the broadcast property of wireless transmission. We design an IEEE 802.11-compliant MAC protocol that provides receiver anonymity for unicast frames and offers better reliability than pure broadcast protocol.

REFERENCES

[1] IEEE. std 802.11, 1999 Edition, Wireless LAN Medium Access Control (MAC) and Phyiscal Layer (PHY) Specifications. 1999.

[2] A. S. Tanenbaum. Computer Networks (Third edition). Prentice Hall, 1996.

[3] M. T. Sun, L. Huang, A. Arora, and T. H. Lai. Reliable MAC layer multicast in IEEE 802.11 wireless networks. In Proc. of the 31st International Conference on Parallel Processing (ICPP), pages 527–536, Vancouver, Canada, Aug. 2002.

[4] K. Tang and M. Gerla. MAC layer broadcast support in 802.11 wireless networks. In Proc. of the IEEE Military Communication Conference (MILCOM), pages 544–548, Los Angeles, CA, Oct. 2000.

[5] S.-T. Sheu, Y. Tsai, and J. Chen. A highly reliable broadcast scheme for IEEE 802.11 multi-hop ad hoc networks. In Proc. of the IEEE International Conference on Communications (ICC), pages 610–615, New York, NY, Apr. 2002.

[6] W. Si and C. Li. RMAC: A reliable multicast MAC protocol for wireless ad hoc networks. In Proc. of the 33rd International Conference on Parallel Processing (ICPP), pages 494–501, Montreal, Canada, Aug. 2004.

[7] K. Xu, M. Gerla, and S. Bae. How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks? In Proc. of the IEEE Global Telecommunication Conference (GLOBECOM), pages 17–21, Taipei, Taiwan, Nov. 2002.

[8] K. Tang and M. Gerla. MAC reliable broadcast in ad hoc networks. In Proc. Of the IEEE Military Communication Conference (MILCOM), pages 1008–1013, McLean, VA, Oct. 2001.

[9] U. Berkeley, LBL, USC/ISI, and Xerox-PARC. The ns Manual (formerly ns Notes and Documentation). 2003.

[10] J. Tourrihes. Robust broadcast: Improving the reliability of broadcast transmissions on CSMA/CA. In Proc. of the 9th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Boston, MA, Sept. 1998.