An Efficient Security Mechanism to Detect the Packet Droppers in a MANET under Individual and Collusive Adversarial Models

Shirina Samreen
Research Scholar, Dept. of Computer Science
JNTUH College of Engineering
Kukatpally, Hyderabad, A.P., India

G.Narasimha, Ph.D
Associate Prof., Dept. of Computer Science
JNTUH College of Engineering
Nachupally, Kondagattu, Karimnagar, A.P., India

ABSTRACT
Most of the existing security mechanisms for detecting the packet droppers in a mobile ad hoc network generally detect the adversarial nodes performing the packet drop individually wherein false accusations upon an honest node by an adversarial node are also possible. In this paper, we propose a security mechanism to detect those nodes performing packet dropping either on their own individually or in collusion such that they cannot evade detection and no false accusations are possible. The detection of adversarial nodes is done by the source node through the analysis of the reports submitted by all the intermediate nodes on the source to destination paths. The composition of the report from each of the intermediate nodes involves certain pre-computed hash values which act as acknowledgments from each receiver node (successor) to the forwarder node (predecessor) and also a secure proof through which each intermediate node claims the packets which have been received within a communication session. The proposed mechanism has minimum communication and computational overhead since the secure proof is based upon a hash computation and report submission is secured through symmetric cryptographic primitives. The report analysis process ensures that evading the detection is not possible even in collusive adversarial model.

General Terms
Mobile Ad hoc Networks (MANETs), Routing Protocols, Attacks on MANET, Secure Routing.

Keywords
Packet droppers, Colluding adversaries, Reports, Secure proof, Onion hash.

1. INTRODUCTION
The inherent characteristics of a MANET create a lot of security vulnerabilities on the routing mechanism as well as on the data transmission activity. One of the most challenging attacks is the packet drop attack after the establishment of secure route because of the multi-hop communication wherein the transmission of packets requires the nodes to relay the packets of the other neighbouring nodes. Packet dropping / Packet forwarding misbehaviour in a MANET can occur because of the rational as well as irrational / malicious reasons wherein the rational packet dropping may occur either due to selfish nature of the nodes in a MANET to preserve their battery power by not involving in the relay of other node's packets or congestion in the network or bad channel condition and malicious packet dropping occurs when a node has been compromised by an adversary and wants to disrupt the network performance by simply dropping the packets without forwarding them.

The problem of packet forwarding misbehaviour in a MANET can be addressed using the following two strategies:

- Cooperation Stimulation Strategy
- Cooperation Enforcement Strategy

In Cooperation stimulation mechanisms, the intermediate nodes are rewarded with credits for relaying other's packets and the communicating end nodes are charged for using the packet forwarding services of the intermediate nodes. The intermediate nodes usually compose payment reports / receipts which are undeniable proofs of their packet relaying service which contain the identities of payers and payee and the payment amount. These proofs are cryptographically protected from forgery. These receipts are processed by a trusted centralized unit called Accounting Center (AC) or Trusted Party (TP) with which a connection is established periodically during which the accumulated receipts are processed. The drawback of most of these schemes is that they need a tamper resistant hardware to prevent the manipulation of credit related information or usage of public key cryptography to secure the payment data.

Cooperation Enforcement Mechanisms may be categorized as monitoring based approaches, acknowledgement based approaches and probing based approaches. These mechanisms have the data transmission activity attached to yet another module to detect the packet droppers. The misbehaviour detection module can be based upon promiscuous neighbourhood monitoring which places an additional burden on all the nodes to monitor the behaviour of neighbouring nodes. Acknowledgement based schemes may also be used for detecting the misbehaviour but it may result in additional traffic and finally probing based schemes may be used to locate the packet dropper on the source to destination path. The probing has to be done in an unobtrusive way to ensure that the adversary does not evade detection.

In this paper, we propose a security mechanism wherein each node on the source to destination path always has a report comprising of a secure proof of all the packets it received as well as the ones it forwarded which is always verifiable by the source node that is always trusted and responsible for detecting the adversarial nodes. The composition of the secure proof ensures that minimum computational and communication overhead is incurred.

The paper is organized as follows. Section 2 gives the related work in the concerned area. Section 3 describes the details of

the proposed security mechanism describing the assumptions, the construction of acknowledgement report, the report analysis and the adversarial models. Section 4 presents the conclusion and future work.

2. RELATED WORK

In credit based mechanisms like [1] and [2] the usage of credits called nuggets is done which will be awarded for a node for packet forwarding. Two models have been proposed known as Packet Purse Model and Packet Trade Model. In both these models, each intermediate node receives nuggets for packet forwarding activity which it requires for transmitting it's own data packets. Hence every node intends to increase it's nugget count for which it performs packet forwarding for other nodes. Another approach known as Sprite proposed by Zhong et al [3] uses a central server reachable through internet called Credit Clearance service which either charges or credits the nodes for packet forwarding activity depending on whether they have provided the service to others or utilized the service from others. The drawback of these techniques is that, they need tamper-resistant hardware to prevent the nodes from modifying the credit-related information. These are called as Incentive protocols which use credits to stimulate the selfish nodes for cooperation but these protocols have to secure the payment for which they rely on heavy weight public-key cryptography. Many light-weight secure incentive protocols have been proposed like ESIP (Efficient and secure cooperation incentive protocol) [4] which uses light weight hashing operations on all the packets following the first packet, RACE (Report based Payment Scheme) [5] which incurs no cryptographic processing as the inconsistencies in the reports are used as a basis for misbehaviour detection, and TRIPO (Thwarting the Rational and Irrational Packet Dropping Attacks) [6] which involves a monitoring technique to measure the nodes' frequency of dropping packets by examining the payment receipts rather than medium overhearing.

In monitoring based approaches like [7], [8] and [9] each node in the MANET has to monitor the forwarding activity of their neighbourhood wherein the metrics pertaining to inflow and outflow traffic of a neighbouring node are monitored. Acknowledgement based approaches like [10] and [11] require sending of acknowledgements either by an intermediate node or the destination node to it's upstream neighbours as a proof of packet reception. Probing based approaches like [12] and [13] probe the source to destination path for the identification of packet droppers which involves sending traffic onto a network to sample it's behaviour. The traffic can be in the form of simple probe packets or complex test transactions which is used to obtain metrics pertaining to end-to-end communication points such as latency, loss, and route availability.

Packet dropping attack which involves an adversary dropping the packet in such a way that it evades detection and can cause a legitimate node to come under suspicion is termed as Stealthy Packet Dropping Attack [14]. This attack can be countered by having two additional requirements over baseline monitoring of having the neighbours maintain additional information about the routing path and to have some additional checking responsibility to each neighbour. An approach which provides a resource efficient accountability for node misbehaviour in MANET based upon random audits is the REAct system [15]. It can be used to locate individual misbehaving nodes that perform packet drop attack. It uses bloom filters as node behavioural proofs for the forwarding activity but it fails under colluding adversarial model. An acknowledgement based scheme is the 2ACK technique proposed by kejun Liu [16] wherein the misbehaviour is detected based upon number of packets which missed the acknowledgments. In [17], the source node expects acknowledgements from the destination as well as the intermediate nodes. Based upon the missing acknowledgements, the neighbourhood nodes are required to promiscuously monitor the forwarding activity to detect the packet droppers. A drawback of these techniques is that a lot of network traffic is created in the form of acknowledgement packets.

3. PROPOSED SECURITY MECHANISM

The design of proposed security mechanism intends to perform the detection of packet droppers in the presence of adversaries which may be individual nodes acting on their own or colluding nodes working in cooperation to drop the packets in such a way that minimum overhead is incurred unlike most of the existing mechanism based upon acknowledgement packets for each data packet. The transmission of the data packets occurs in the form of sessions each of which involves the continous transmission of a fixed number of data packets (say n) from the source to destination which is followed by a cumulative acknowledgement report. The cumulative acknowledgement report comprises of the feedback from each of the intermediate nodes on the source to destination path about the reception of each of the n data packets for the current session. Based upon analysis of these reports, the source node detects the packet droppers.

3.1 Assumptions

The proposed security mechanism addresses the packet forwarding misbehaviour after the establishment of a secure route from source to destination. More specifically, it is used to detect the adversarial nodes on the source to destination path which perform packet dropping either individually or by acting in collusion. At the end of the data transmission, the source enters the behaviour monitoring phase wherein it has to receive the reports from each of the intermediate nodes and also the destination which are protected cryptographically. The source performs the analysis of these reports and looks for inconsistencies to decide about the adversarial nodes on the source to destination path. The following are the assumptions of the proposed mechanisms:

- Only the source and destination are trusted nodes during the data transmission.
- Each of the communication links are bidirectional.
- Each communication session corresponding to data transmission after the establishment of a secure route involves transmission of n data packets between a source node S and the destination node D. The value of n is predefined and known to all the nodes in the network.
- The successive data packets within a communication session are assigned consecutive sequence numbers.
- The source buffers all the n packets corresponding to one communication session until the misbehaviour detection scheme has completed.
- The source shares a symmetric key with each of the intermediate nodes and also with the destination.

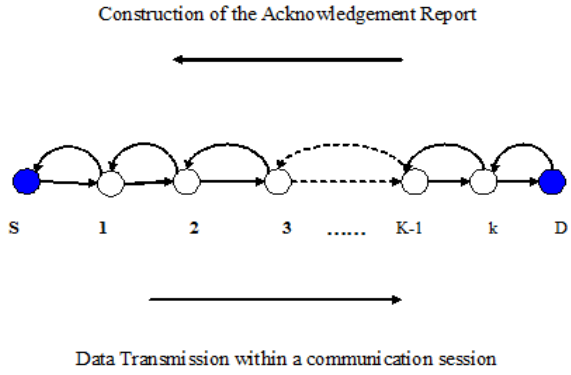
3.2 Security Mechanism

Once a secure route has been established between the source and destination, consisting of k intermediate nodes, the source generates n random numbers r_1, r_2,…. r_n (assuming n packets in a communication session) and uses a hash function h to compute $h(r_1)$, $h^2(r_1)$, $h^3(r_1)$…… $h^k(r_1)$, $h(r_2)$, $h^2(r_2)$, $h^3(r_2)$…… $h^4(r_2)$,….. $h(r_n)$, $h^2(r_n)$, $h^3(r_n)$…… $h^k(r_n)$. These values are distributed among the intermediate nodes by encrypting them with the symmetric keys of each of the intermediate nodes. Assuming that the intermediate nodes are named as 1, 2, 3…..k , then the message for node 1 is $E(K_{S1}, h^k(r_1)| h^k(r_2)| h^k(r_3)|…… h^k(r_n))$, for node 2 the message is given as $E(K_{S2}, h^{k-1}(r_1)| h^{k-1}(r_2)| h^{k-1}(r_3)|…… h^{k-1}(r_n))$, likewise the hashed values in the decreasing order are given to the intermediate nodes. Hence the message for node k is $E(K_{Sk}, h(r_1)|h(r_2)|h(r_3)|…… h(r_n))$ where K_{S1}, K_{S2}, K_{S3}, ... , K_{Sk} are the symmetric keys which the source shares with the intermediate nodes 1, 2, 3,….,k respectively. The data transmission activity is followed by a misbehaviour detection scheme based upon the analysis of the reports gathered from the intermediate nodes. The report consists of a secure proof which indicates those packets received by a node within a session along with an n bit flag indicating the packets which have been received / not received from it's upstream neighbour in the path. An analysis of the inconsistencies in the reports of successive intermediate nodes allows the source to arrive at a decision about the packet forwarding behaviour of each of the intermediate nodes.

Each of the intermediate nodes compose a report after receiving a data packet from the upstream neighbour. The report consists of three parts: a secure proof which indicates the packets which were actually received, an n bit flag which provides information about the received and missed packets within a session comprising of n packets and an acknowledgement values for each forwarded packet from the downstream neighbour after the packet reception. The bit flag and the secure proof have to be consistent with each other failing which a node is considered as cheating / adversary.

The secure proof is actually an onion hash of all the successive packets received by an intermediate node. The main idea behind using an onion hash is to reduce the communication and processing overhead. The n bit flag which consists of n bits is formed in such a way that it is initialized to all zeros. The reception of a packet with x as the sequence number will result in marking the bit position x to 1 (bit positions are considered to be marked from 1 to n starting from left). Each forwarding intermediate node i (1<=i<k) upon forwarding a packet with sequence number j, expects an acknowledgement value from it's downstream neighbour node i+1 in the form of value $h^{k-i}(r_j)$ so that it can verify the correctness of the acknowledgement through it's own hash value $h^{k-i+1}(r_j)$ by checking that $h^{k-i+1}(r_j) = h(h^{k-i}(r_j))$. An intermediate node can send an error message to the source whenever a wrong acknowledgement value is received after a fixed number of retransmissions.

At the end of a communication session, the destination has to send an acknowledgement report which consists of it's n-bit flag each bit of which indicates the packets which have been received / missed. Apart from the n-bit flag, the acknowledgement report comprises of several other components which include the concatenation of the reports from all the intermediate nodes on the path from source to destination. These reports are protected from manipulation by any adversarial nodes on the path by having a chained HMAC computed using the symmetric key of each intermediate node appended to the part of the report composed so far. Figure 1 below shows the hop by hop construction of acknowledgement report. As the source is aware of the intermediate nodes on the source to destination path and the symmetric keys which they share with the source, it recomputes the chained HMAC by using the individual reports of each of the intermediate nodes found in the acknowledgement report received from the destination. If the computed HMAC is the same as the one received in the ack report, it accepts the report as valid, otherwise it is rejected.



At node k
$[nflag_D, Rep_k, HMAC_k]$
$HMAC_k = HMAC(K_{Sk}, nflag_D|Rep_k)$

At node k-1
$[nflag_D, Rep_k, HMAC_k, Rep_{k-1}, HMAC_{k-1}]$
$HMAC_{k-1} = HMAC(K_{Sk-1}, nflag_D|Rep_k|HMAC_k|Rep_{k-1})$

At node 1 → Final Acknowledgement Report submitted to S
$[nflag_D, Rep_k, HMAC_k, Rep_{k-1}, HMAC_{k-1}$…… $Rep_1, HMAC_1]$
$HMAC_1 = HMAC(K_{S1}, nflag_D|Rep_k|HMAC_k|Rep_{k-1}|HMAC_{k-1}|$…..$|Rep_1)$

Fig 1: Hop by Hop Construction of the Acknowledgement Report on the reverse Source to Destination Path

After verifying the integrity of the acknowledgement report, the source proceeds for the extraction and the verification of the individual reports from each of the intermediate nodes. This is followed by the analysis of these reports to arrive at a decision about the forwarding behaviour of each of the intermediate nodes. Specifically, it aims to locate the nodes which may be involved in the packet drop through a broken link at the forwarding level. At the end of analysis, the nodes may be classified into one of the three categories as honest, dropper, and cheater. A node which forwards all the packets which it receives is termed as an honest node. The nodes which drops the packet without forwarding it to it's successor on the path is termed as a dropper. A node whose report shows inconsistency in the secure proof and the n-bit flag is termed as a cheater.

3.2.1 Report Analysis

The analysis of the individual reports from each of the intermediate nodes is done as follows: In the first step, for each of the intermediate nodes, the secure proofs are verified by computing the onion hash upon those packets which are claimed by the node as received. The n-bit flag is used to find which packets have been received and the onion hash is computed upon those packets by the source node and the computed hash is compared against the received hash in the form of a secure proof. If any inconsistencies are found, then the node is termed as a cheater and it's reputation is updated accordingly.

In the second step, after discarding the reports of all the cheaters from consideration, the analysis proceeds with the reports of remaining nodes. Specifically, the n-bit flags of all the non-cheater intermediate nodes are arranged in the order in which they appear in the source to destination path. Those bit positions which are zero in the destination's n-bit flag are examined. Let the first intermediate node whose n-bit flag has a zero in the same position is called N. If all the remaining intermediate nodes downstream to N have a zero in that bit position, then it represents a packet drop by a forwarding level link break through a link between N and it's upstream neighbour say M. In such a packet drop, one of the nodes associated with the broken link have actually resulted in the packet drop. The exact node which has performed the packet drop can be found by looking into the acknowledgement field of the reports of each of the intermediate nodes.

3.2.2 *Colluding Adversarial Model*

Apart from the droppers which represent a packet drop performed by an individual adversarial node, we also consider a packet drop performed by colluding adversaries. In the colluding adversarial model which we consider, two non-consecutive intermediate nodes on the source to destination path collude in such a way that, the upstream one drops the packet and the other downstream one illegitimately procures the secure proof from the upstream colluding node so as to create an impression that the honest intermediate nodes in between the non-consecutive colluding intermediate nodes have actually dropped the packets. This type of attack can be addressed by using the acknowledgement scheme wherein each intermediate node's acknowledgement values are checked. Let us say M1 and M2 represent the two non-consecutive colluding adversaries and M1 is upstream node which is actually dropping the packets. The node M2 colludes with the node M1 in such a way that M1's misbehaviour is evaded by appropriately manipulating the report contents. Figure 2 below illustrates the said colluding adversarial model.

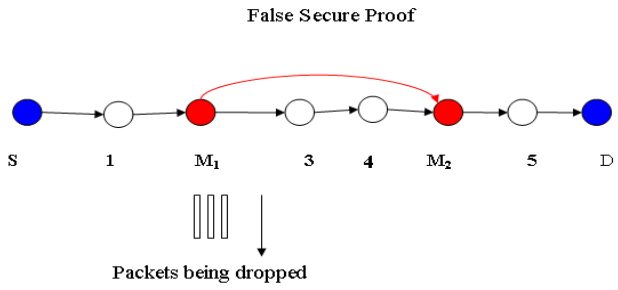


Fig 2: S and D represent the source and destination nodes respectively, M1 and M2 represent the colluding adversaries, 1, 3, 4 and 5 represent the honest intermediate nodes on the source to destination path.

This type of attack has the reports where, for certain bit positions which are zero in the destination's report, the value is 1 in M1's report, a 0 in the reports of nodes in-between M1 and M2 and a 1 in the report of M2. Two cases arise as follows:

Case 1: M1 and M2 are honest

If M1 and M2 are honest in their report composition, then both of them should also have proper acknowledgement value from their respective successors which indicates that, all the successive nodes in between M1 and M2 should be declared as cheaters.

Case 2: M1 and M2 are cheaters

This type of attack is intended to falsely blame the in-between nodes as misbehaving at the cost of getting M2 termed as a packet dropper since the proper ack value in it's report will be missing. Such an attack can be countered by using the acknowledgement values of all the packets which M1 claims to have forwarded. If M1 has dropped the packets, it's report will miss the acks of all such packets. Hence M1 and M2 will be declared as colluding adversaries who are involved in a packet drop.

4. CONCLUSION AND FUTURE WORK

The proposed security mechanism efficiently addresses the packet dropping attack carried out by either an individual node or by multiple nodes acting in collusion. It incurs minimum computational overhead since the secure proof is based upon a hash computation and report submission is secured through symmetric cryptographic primitives. Our future work aims at enhancing the proposed security mechanism for countering a more enhanced colluding adversarial model involving a set of consecutive nodes on the source to destination path acting as colluding adversaries. We plan to simulate the proposed security mechanism to analyze it's efficiency under the different adversarial models using the ns-2 network simulator.

5. REFERENCES

[1] L. Buttyán, and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," Mobile Net works and Applications, 8(5), pp. 579-592, 2003.

[2] M. Jakobsson, J.-P. Hubaux, and L. Buttyan, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," in Financial Crypto, 2003.

[3] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple cheat-proof, credit-based system for mobile ad-hoc networks," in IEEE INFOCOM, pp. 1987-1997, 2003.

[4] Mohamed Elsalih Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks", IEEE Transactions On Vehicular Technology (IEEE TVT), Vol. 60, No. 8, pp. 3947-3962, 2011

[5] M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use of public-key cryptography for multi-hop wireless networks", IEEE Transactions on Mobile Computing (IEEE TMC), vol. 10, no. 7, pp. 997-1010, July 2011

[6] Mohamed M. E. A. Mahmoud and X. Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, pp. 209–224, Feb 2013

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual international Conference on Mobile Computing and Networking (MOBICOM), pp. 255-265, 2000

[8] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad-hoc networks by reputation systems," IEEE communications Magazine, pp. 101-107, 2005

[9] P. Michiardi, and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of IFIP Joint Working Conference on Communications and Multimedia Security, pp.107-121, 2002

[10] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur. 10(4), 1-35, 2008

[11] Panagiotis Papadimitratos *, Zygmunt J. Haas,"Secure message transmission in mobile ad hoc networks", Proceedings of the 2nd ACM workshop on Wireless security, WiSe 2003

[12] M. Just, E. Kranakis, and T. Wan, "Resisting malicious packet dropping in wireless ad-hoc networks using distributed probing," in Proceedings of ADHOC-NOW '03, Oct. 2003

[13] I. Avramopoulos and J. Rexford, "Stealth Probing: Efficient Data-Plane Security for IP Routing," In Proc. USENIX Annual Technical Conference, Boston, MA, May 2006

[14] Khalil And Bagchi: Stealthy Attacks In Wireless Ad Hoc Networks: Detection And Countermeasure 2011 IEEE Transactions On Mobile Computing, Vol. 10, No. 8, August 2011

[15] W. Kozma, and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009

[16] K. Liu, J. Deng, P. Varshney, K. Balakrishnan, "An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, 6(5), pp. 536550, 2007.

[17] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.