A Collusion-resistant Acknowledgement-based Secure Intrusion Detection System for MANETs

Ms. Anjaly G D, Ms. J C Kavitha

Abstract— MANETs are based on wireless multi-hop communication. To ensure correct operation, nodes need to cooperate and forward messages from other nodes. However there can be misbehaving nodes that can silently drop packets. Such misbehaviors can be either an individual node misbehavior or misbehavior of nodes in collusion. In this paper, a new approach is proposed to identify and mitigate the packet dropping due to individual node misbehavior and collusion.The scheme also avoids the issue of forged acknowledgements. This secure collusion-resistant acknowledgement-based scheme, called CRACK is introduced based on DSR protocol. Simulation results are presented to estimate the performance of the proposed scheme and compare it with the other methods.

1 INTRODUCTION

ONE of the key benefits of wireless networks is its ability to allow different parties to communicate while maintaining their mobility. However, such a communication is restricted to the range of transmitters. This means that two nodes cannot communicate when the distance between them is more than the communication range of their own. Mobile Ad-hoc Networks (MANET) resolves this issue by allowing the in-between parties to convey data transmissions. In MANETs the range of the network is improved by active cooperation of the participating nodes. Nodes in the network perform routing and forward messages on behalf of the other nodes. MANET can form a self-organized and self-maintained network without the help of a centralized infrastructure, which is often not possible in mission-critical applications like military clashes or disaster recovery. Minimal set-up and quick deployment make MANET equipped to be used in emergency situations where an infrastructure is unavailable or where it is impractical to install- in scenarios like natural or human-induced disasters, military clashes, and medical emergency situations.

Owing to these special characteristics, MANET is extensively implemented in the industry. On the other hand, as MANET is popular amongst mission-critical applications, security of MANET is vital. Unfortunately, the wireless medium and remote distribution of MANET make it susceptible to different types of attacks. For example, as the nodes miss physical protection, malicious attackers can effortlessly capture and compromise nodes to realize attacks. The routing protocols of MANETs assume that all nodes are honest and helpful. But such collaboration cannot be assumed in general.Hence Intrusion Detection Systems(IDS) are very important.

- *Ms. Anjaly G.D is currently pursuing masters degree program in Computer Science and engineering, Meenakshi College of Engineering, Chennai, India. E-mail: anjalydiv@gmail.com*
- *Ms. J.C. Kavitha is currently working as Head of the Department, Department of Computer Science and engineering, Meenakshi College of Engineering, Chennai, India. E-mail: jck_kavitha@yahoo.co.in*

It can be beneficial for nodes to misbehave during the process of forwarding a packet, e.g. to save resources such as battery power. A frequent attack is to drop messages of other nodes. Such nodes that misbehave so as to save its energy or battery power are termed as selfish nodes. Such misbehavior can be either an individual node misbehavior or misbehavior of nodes in collusion.

Colluding misbehaving nodes are able to conceal the actions of each other in order to prevent detection of misbehavior. This misbehavior is described in detail in Section 3.

In this paper, the problem of routing misbehavior in the routing protocols is addressed. Specifically, we simultaneously address the problem of identifying misbehavior nodes that cooperate in routing phase, but refuse to forward data packets to a destination and also collusion attacks.The method also addresses the issue of forged acknowledgements. The proposed Intrusion Detection System is based on DSR protocol. In this system, CRACK [15] is used to detect the misbehavior node on the path that drops the packets.

The paper is structured with related work in Section 2. Assumptions and problem definition is explained in section 3. Section 4 describes the proposed scheme. Section 5 presents the performance evaluation. Section 6 deals with the conclusion and future work.

2 RELATED WORK

In MANET, a variety of techniques have been proposed to thwart routing misbehaviors and to reduce the effects of routing misbehaviors. These schemes can be usually classified into three categories: credit-based schemes, reputation-based schemes and acknowledgement-based schemes.

2.1 Credit-based Scheme

The concept of credit-base schemes is to provide incentives so as to promote nodes to forward data packets using virtual currency or other payment schemes. Nodes receive rewards by providing services to other nodes. Similarly, a node must pay other nodes if they forwards packets sent by that node.

Buttyan and Hubaux (2003)[3] propose this scheme where

nodes charge for delivering services and compensate for receiving a service. In their protocol, every node keeps a counter, called a nuglet counter, in a tamper-resistant hardware module. The counter is decremented when the node sends its own packets, and it is incremented when the node forwards packets sent by other nodes. The counter must have a positive value or else the node will not be permitted to send its own packets. Therefore, each node is encouraged to supply forwarding services.

Zhong et al. (2003) [9] propose another credit-based scheme, called Sprite. The features of this scheme do not require tamper-proof hardware at any node. In Sprite, nodes maintain receipts of the forwarded and received messages. Later, nodes provide their receipts to the Credit Clearance Service (CCS), and CCS decides their charge and credit. Nodes should have enough forwarding credits so as to send their own messages.

Wang and Li (2006) [12] propose a strategy-proof pricing scheme for wireless ad-hoc networks. Every node has a true cost and a declared cost. Depending on the declared cost, source calculates the Least Cost Path (LCP). The payment made to the node in LCP is declared cost plus the difference between the cost of the LCP without using this node and the cost of the LCP. If the node is not in LCP, payment to it is zero. This scheme pays every node more than its declared cost so as to avert it from lying.

Anderegg and Eidenbenz (2003) [11] proposed the Ad-Hoc VCG protocol which was a reactive routing protocol in MANET. This protocol uses a game-theory model to guard against selfish nodes. This protocol assumes that there is a central bank that processes all monetary transactions and each node has its own bank account. During the route discovery, it computes the most energy-efficient path that links the source to the destination. During the data transmission phase, the data packets are transmitted along the least energy path. The source node then owes all intermediate nodes a payment.

Eidenbenz et al. (2008) [13] propose COMMIT, a protocol for route discovery and for forwarding packets in ad-hoc networks. VCG payment scheme is the base of the COMMIT protocol. It improves the drawbacks of the Ad Hoc-VCG while maintaining the advantages of honest and energy-efficient routing. This protocol allows the source to act advantageously and compute costs using nodes in order to decrease the message complexity.

Because credit-based schemes usually require tamper proof hardware or payment systems; we focus our efforts on reputation-based schemes instead.

2.2 Reputation-based Scheme

In reputation-based schemes, nodes identify and declare misbehavior of a suspicious node. When a declaration is heard, nodes detach the misbehaving node from the network.

Marti et al. (2000) [7] propose a scheme to alleviate routing misbehavior in MANET. It contains two main modules: watchdog and pathrater. The watchdog module detects misbehaving nodes and the pathrater helps the routing protocol to stay away from these nodes. By overhearing, nodes verify whether the next-hop node faithfully forwards the packets or not. Though the throughput is increased by 17% when 40% of nodes are misbehaving, the overhearing technique may still fail to detect misbehaving nodes under certain situations, such as: ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, collusion and partial dropping.

Buchegger and Boudec (2002) [2] propose a protocol, termed CONFIDANT that works as an extension to a reactive routing protocol in MANET. CONFIDANT is based on selective altruism and utilitarianism, and it has four components: the monitor, the reputation system, the path manager, and the trust manager. Each node watches the behavior of its next-hop neighbors. In case of a suspicious event, the information is passed to the reputation system. Based on the frequency of detection, the reputation system updates the suspected node's rating. If the rating becomes intolerable, the information is provided to the path manager. The path manager removes the intolerable node from the route cache. Afterwards, the trust manager sends an ALARM message to caution the other nodes. Since the monitor component also makes use of the overhearing technique, the CONFIDANT scheme also suffers from the same issues as the watchdog scheme.

2.2 Acknowledgement-based Scheme

Balakrishnan, Deng, and Varshney (2005) [1] propose a network layer acknowledgment-based scheme, called TWOACK, to identify misbehaving nodes. In this scheme, each node observes the behavior of its next-hop using acknowledgments instead of overhearing the next node's behavior. The TWOACK scheme could provide a solution to some of the issues related to the overhearing technique, such as ambiguous collisions, receiver collisions, and limited transmission power. TWOACK is an initial version of the 2ACK scheme.

Liu et al. (2007) [14] propose a new 2ACK scheme that also make use of acknowledgments like the TWOACK scheme. There are some differences between 2ACK and TWOACK schemes. First, destination node in the 2ACK scheme only sends a fraction of 2ACK packets, but the TWOACK scheme sends all the TWOACK packets for each data packets. 2ACK can obtain superior performance than TWOACK for its fractional acknowledgment packets. Second, the 2ACK scheme uses an authentication scheme to prevent the 2ACK packet from being modified. Though throughput is efficiently increased in the 2ACK scheme, it cannot resist collusion attacks and malicious alarms.

H. M. Sun et al. [8] proposed a scheme, called NACK, which uses an acknowledgment-based method and comparison of timestamps to resist the collusion attacks. The NACK scheme like the TWOACK scheme, sends 2-hop acknowledgment in the reverse direction to confirm that the intermediate node cooperates in the packet forwarding, but the NACK scheme uses timestamps comparison and an additional route between source and destination, to detect misbehavior node (not only misbehavior link). Each node when receives a packet should send a NACK packet and the destination node should send a delivery packet to the source node on the second route. The shortcomings of the scheme were that it made an assumption that time synchronization exists in MANET and had an additional overhead when compared to the DSR routing protocol.

3 Assumptions and Problem Definition

3.1 Assumptions

In the proposed scheme, we assume that the link between each node in the network is bi-directional. For each communication process, we assume that the source node and destination node are not malicious. The packet dropping node is assumed to show selfish behavior-drops all data packets while taking part in routing process.

3.2 Problem Definition

MANETs are based on wireless multi-hop communication. Messages are exchanged between the source and the destination by using hop-by-hop forwarding through the in-between nodes. To ensure the correct operation of the routing protocol, the nodes need to collaborate and forward messages of other nodes based on the protocol specification. However, from an opportunistic node's perspective it might be better to mutely drop messages of other nodes or stay away from being part of the link between two end systems so that it can save its computational power, energy and bandwidth. Such misbehavior will be individual node misbehavior.

However, there could be presence of colluding misbehaving nodes as well. Messages are received from the misbehaving node/subnet, but dropped as soon as no non-malicious/good node is able to observe the routing behavior. Thus in collusion, two or more consecutive misbehaving nodes cooperate to mount a sophisticated attack.

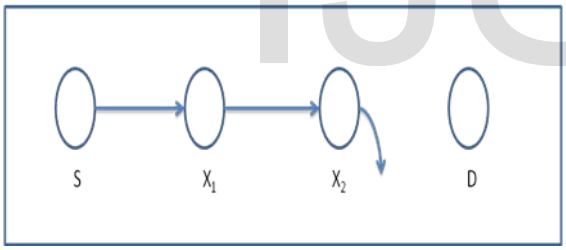

Fig. 2: Colluding nodes X_1 and X_2

The detailed explanation of collusion is provided using the above Fig. 2.Here the source S is sending a packet to destination D via the nodes X_1 and X_2.S forwards the packet to X_1 and X_1 forwards the packet to X_2 but X_2 drops the packet. Here both X_1 and X_2 are said to be maliciously colluding. The behavior of X_1 and X_2 can be generalized as:

- X_1 forwards all packets received from non-malicious/good nodes (in this case to X_2).
- X_2 does not forward packets which were not generated by malicious nodes, but received from a colluding malicious node.
- X_1 is able to detect the misbehavior of X_2. But since X_1 and X_2 collude, X_1 silently accepts the misbehavior and does not report it, which thus goes unnoticed for the benign nodes S and D.

One hop mechanisms that detect forwarding misbehavior like Watchdog that was based on overhearing (proposed by Marti et al.) could not detect this collusion because to source S, X_1 is a genuine node as it forwards packets correctly to X_2 and X_1 though it knows that X_2 drops packets does not report it back to the source S.

An attacker can also forge the acknowledgements thereby providing a wrong interpretation for a good/benign node as a colluding node.

4 Scheme Description

In this section, we describe our proposed scheme in detail. The scheme uses a special packet called CRACK which will be like a normal data packet but which contains the id of the node to which packet is sent to and the packet will be encrypted using RSA scheme. RSA is a public key encryption scheme-the sender encrypts data using the public key and the receiver decrypts data using the private key. The justification for using RSA in our proposed scheme is receiver authentication.For avoiding forged acknowledgements; all acknowledgements are digitally signed using DSA (Digital Signature Algorithm).

The source node starts a timer, and sends an encrypted CRACK packet to the destination, i.e., the CRACK packet will have destination node ID and will be encrypted using RSA. Only destination node will be able to decrypt this packet, and if it can decrypt this packet and cross-check that packet has its own node ID, it can send an acknowledgement back to the source. If the source receives an acknowledgement from destination within the timeout limit, it means there are no misbehaving nodes between source and the destination. If otherwise, keeping a timer, source will again send an encrypted CRACK packet to the node before the destination node and so on till it receives an acknowledgement. Now, the node which gives an acknowledgement in this case would be the misbehaving/packet dropping node.

The advantage of this scheme is that it detects packet dropping due to individual node misbehavior as well as due to collusion. Thus, if the acknowledgement is not from destination node, it is from a misbehaving node. As per colluding nodes, it processes the packet first, sends an acknowledgement if condition is satisfied and then drops the packet.

In order to distinguish different packet types, we included a 1-b packet header in our proposed scheme. According to the Internet draft of DSR [6], there is 6 b reserved in the DSR header. In our proposed scheme, we use 1 b of the 6 b to flag different types of packets. Details are listed in Table 1.

TABLE 1
PACKET INDICATORS

Packet Type	Packet Flag
General packet	0
CRACK packet	1

The proposed scheme is embedded within DSR protocol.DSR protocol is divided into route discovery and route

maintenance. Thus in CRACK scheme also, the source node first searches its local knowledge base to see if a path already exists to the destination. If so the same path will be used for further communication, else the source node initiates a DSR routing request to find a path to the destination. This path would be used for CRACK scheme.

Now once the source receives the acknowledgement from the misbehaving node, it would be aware of the misbehaving node. So as to mitigate the packet dropping, the source node sends an alarm to all other nodes in the same network. The alarm contains the misbehaving node ID. When other nodes receive this alarm, the reported node will be directly banned from accessing the network.

5 Performance Evaluation

In this section the simulation results for performance evaluation is presented. First, the simulation methodology and performance metrics are explained and then, the simulation results are given.

5.1 Simulation methodology and performance metrics

In the simulations, a version of Network Simulator (NS-2.34) that includes wireless extensions developed by the CMU Monarch project group is used. The DSR module is modified to simulate the proposed scheme and misbehavior nodes. The IEEE 802.11 MAC was used. The simulation parameters are summarized in Table 2. User Datagram Protocol traffic with constant bit rate is implemented. The assumptions explained in section 3.1 are considered in the simulations.

Regarding the RSA scheme, we adopted an open source C++ cryptographic library named Botan. This library is locally compiled with GCC.

TABLE 2
Simulation Parameters

Number of nodes	50
Transmission range	250
Simulation area (m^2)	1000X1000
Simulation time (s)	100
Data packet size (byte)	512
Traffic rate (kbps)	4
Number of CBR sessions	10
Number of misbehavior nodes (percent)	0, 2, 4, 6, 8 and 10

The following metrics are used to calculate the performance of the proposed scheme with regard to UDP traffic:

- **Packet Delivery Ratio (PDR)**: The ratio of the number of data packets received by the destination to the number of data packets sent by the source.
- **Routing Overhead (RO)**: The ratio of the amount of routing related packets (RREQ, RREP, RERR and CRACK Acknowledgement) to the amount of data packets. Both forwarded and transmitted packets are counted.

5.2 Simulation results for packet delivery ratio

In below Fig. 3, we compare the packet delivery ratio (PDR) of the proposed scheme and the original DSR protocol as a function of misbehavior ratio (MR). The MR ranges from 0 (all of the nodes are trustworthy) to 0.1 (10% of the nodes are misbehavior). The misbehavior simulated includes both individual misbehavior as well as misbehavior due to collusion in presence of forged acknowledgements.

From this figure we observe that increasing the number of misbehavior nodes reduces the packet delivery ratio. As seen, the proposed method has done a much better job in packet delivery compared to the DSR method.

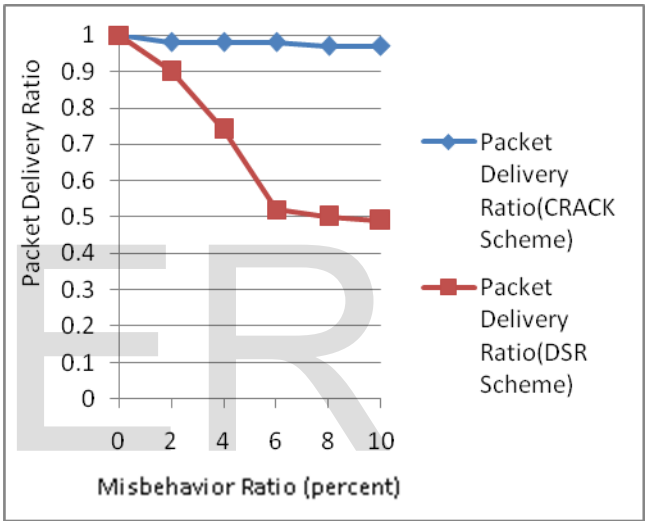

Fig. 3: Packet Delivery Ratio as a function of Misbehavior Ratio (percent)

5.2 Simulation results for routing overhead

Fig. 4, compares the routing overhead (RO) of the proposed scheme and the original DSR protocol as a function of misbehavior ratio (MR). The misbehavior simulated includes both individual misbehavior as well as misbehavior due to collusion in presence of forged acknowledgements.

The higher routing overhead in the proposed scheme is due to the transmission of extra acknowledgment packets, while these packets are not transmitted in DSR. Use of encryption (RSA scheme) and digital signature using DSA also increases the overhead.

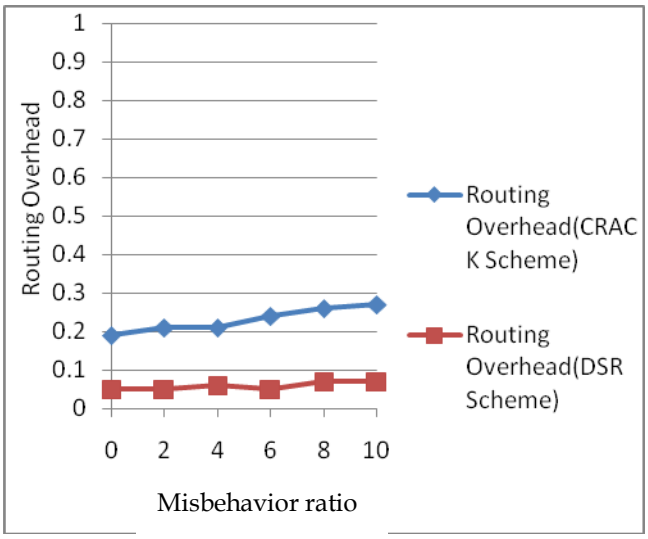

Fig. 4: Routing Overhead as a function of Misbehavior Ratio (percent).

6 Conclusion And Future work

Packet-dropping attack has always been a key threat to the security in MANETs. Collusion is another severe risk that relies on node collaboration. Collusion reduces the packet delivery ratio but is comparatively difficult to detect than packet dropping by individual nodes. In this research paper, we have proposed a novel scheme specially designed for MANETs to detect individual node misbehavior as well as collusion.The scheme also addresses the issue of forged acknowledgements.

Our simulation results show that the proposed scheme is able to tackle individual node misbehavior and collusion effectively in presence of forged acknowledgements and results in an improved packet delivery ratio.

Decreasing the additional overload due to encryption and digital signature and testing the performance of the proposed system in real network environment instead of software simulation will be considered in the future.

References

[1] K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack: Preventing Selfishness in Mobile Ad hoc Networks," In WCNC 2005, pages 2137-2142, 2005.

[2] S. Buchegger and J. Y. L. Boudec,"Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes: Fairness in Dynamic Adhoc Networks," In MobiHOC 2002, pages 226-236,June 2002.

[3] L. Buttyan and J.P. Hubaux,"Stimulating Cooperation in Self-organizing Mobile Ad-hoc Networks,"ACM/ Kluwer Mobile Networks and Applications, 8(5), pages 579-592, 2003.

[4] CP. Chang, JC. Lin and F. Lai,"Trust-group-based Authentication Services for Mobile Ad hoc Networks," In International Symposium on Wireless Pervasive Computing (ISWPC), 06, pages 37–40, January 2006.

[5] T. Chen, O. Mehani and R. Boreli,"Trusted Routing for VANET," In International Conference on Intelligent Transport Systems Telecommunications (ITST), 09, pages 647-652, October 2009.

[6] D. B. Johnson, D. A. Maltz, Y. C. Hu and J. G. Jetcheva,"The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)," Internet-Draft, February 2002.

[7] S. Marti, TJ. Giuli, K. Lai, M. Baker,"Mitigating Routing Misbehavior in Mobile Ad hoc Networks,"In Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), pages 255–265, August 2000.

[8] H. M. Sun, C. C, H, Chen and Y. F. Ku,"A Novel Acknowledgment-based Approach Against Collude Attacks in MANET," In Expert Systems with Applications, 39, pages 7968–7975, July 2012.

[9] S. Zhong, J. Chen, and Y. R. Yang,"Sprite: A Simple Cheat-proof, Creditbased System for Mobile Ad-hoc Networks," In INFOCOM March 2003, pages 1987–1997, 2003.

[10] The Network Simulator (ns-2), URL: http ://www.isi.edu/nsnam /ns/.

[11] Anderegg, L. and Eidenbenz, S. (2003),"Ad hoc-VCG: A Truthful and Cost-efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents,"In ACM MobiCom (September), 245–259.

[12] Wang, W. and Li, X. Y. (2006).,"Low-cost routing in selfish and rational wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, 5(5), 596–607.

[13] Eidenbenz, S., Resta, G. and Santi, P. (2008),"The COMMIT Protocol for Truthful and Cost-efficient Routing in Ad hoc Networks with Selfish Nodes," *IEEE Transactions on Mobile Computing*, 7(1), 19–33.

[14] Liu, K., Deng, J., Varshney, P. K. and Balakrishnan (2007),"An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANET," *IEEE Transactions on Mobile Computing*, 6(5), 488–502.

[15] Anjaly G.D,J.C Kavitha(2014),"A Collusion-resistant Acknowledgement-based Scheme for Mitigation of Packet Drop in MANETs,"In International Conference on Advances in Computer Science and Information Technology (ACSIT-2014),Vels University,Chennai,India, March 2014