International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Resisting Malicious and Packet Dropping Attacks in the Presence of Collisions in Wireless ADHOC Networks

V.Renugadevi[1], C.Saranya[2], P.Saranya[3], D.Arulanantham[4]
[1,2,3]U.G. Students, [4]Assistant professor, Department of Electronics and communication Engineering, Nandha Engineering College, Erode, Tamilnadu, India

Abstract: ***In wireless ad hoc networks, a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network.In this paper, while observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop.***
Keywords: Cooperative bait detection scheme (CBDS), malicious node, mobile ad hoc network (MANET), packet dropping, secret key transmission.

I. INTRODUCTION

DUE to the widespread availability of mobile devices, mobile ad hoc networks (MANETs), [1] have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations property. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes [12]. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. In black hole attacks a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In a multi-hop wireless network, nodes cooperate in relaying/routing traffic [13]. An adversary can exploit this cooperative nature to launch attacks. In this paper, we detect the malicious node In MANETs; this is especially true given the low physical security of mobile devices [5]. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities [3]. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses. In this paper, our focus is on detecting gray hole/collaborative black hole attacks using a dynamic source routing (DSR)-based routing technique. DSR does not have any detection mechanism, but the source node can get all route information concerning the nodes on the route. In this paper, a mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes. Therefore, some auditing mechanism is needed to verify the truthfulness of the reported information. In [9], another proposed method is prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path (measured in terms of packet delivery ratio and delay) to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining “good” routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead. Our proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detect gray hole / collaborative black hole attacks in MANETs malicious node, so a downstream malicious node does not receive this packet. However, this downstream attacker can still open a back-channel to request this information from the upstream malicious node. When being audited the downstream malicious node can still provide valid proof for the reception of the packet. So packet dropping at the upstream malicious node is not detected. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or unintentional. In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attackers can camouflage under the background of harsh

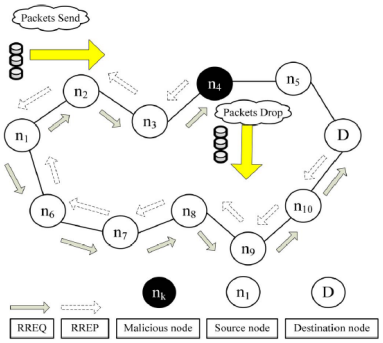

Fig. 1. Malicious node-n4 drops all the data packets

Channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss. For the small number of works that differentiate between link errors and malicious packet drops, their detection algorithms usually require the number of maliciously-dropped packets to be significantly higher than link errors, in order to achieve an acceptable detection accuracy.

II. RELATED WORK

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative black hole attacks. In addition, some of these methods require specific environments [6] or assumptions in order to operate. Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently [14], [15]. In the [7] trust value of a node based on direct observation. Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be classified into the following two categories. The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored.The first sub-category is based on credit systems. A creditsystem provides an incentive for cooperation. The second sub-categoryis based on reputation systems. A reputation system relies on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbors. The third sub-category of works relies on end-to end or hop-to-hop acknowledgements to directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route. The fourth sub-category addresses the problem using cryptographic methods.First hop where the packet is no longer forwarded is considered a suspect for misbehaving.The second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible. All methods mentioned above do not perform well when malicious packet dropping is highly selective. More specifically, for the credit-system-based method, a malicious node may still receive enough credits by forwarding most of the packets it receives from upstream nodes. Similarly, in the reputation-based approach [4], the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop. While the Bloom-filter scheme is able to provide a packet forwarding proof, the correctness of the proof is probabilistic and it may contain errors. For highly selectively attacks (low packet-dropping rate), the intrinsic error rate of Bloom filer significantly undermines its detection accuracy. Our study targets the challenging situation where link errors and malicious dropping lead to comparable packet loss rates.The effort in the literature on this problem has been quite preliminary, and there is a few related works. We model the wireless channel of each hop a random process that alternates between good and bad states. Packets transmitted during the good state are successful, and packets transmitted during the bad state are lost. Detecting malicious packet drops may not be a concern for highly mobile networks, because the fast-changing topology of such networks makes route disruption the dominant cause for packet losses. In this case, maintaining stable connectivity between nodes is a greater concern than detecting malicious nodes. The auditor is responsible for detecting malicious nodes on demand.

In a multi-hop wireless network, nodes cooperate in relaying/routing traffic. An adversary can exploit this cooperative nature to launch attacks.Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such an "always-on" attack has its disadvantages.Attack can detected but malicious nodes are is not identified.Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or unintentional. The proposed mechanism is based on detecting the corre-lations

between the lost packets over each hop of the path.The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (noloss). The benefit of exploiting the correlation of lost packetscan be better illustrated by examining the insufficiency of the conventional method that relies only on the distribution of the number of lost packets. In this case, both ends of the hop will be considered as suspects, i.e., either the transmitter did not send out the packet and the receiver choose to ignore the received packet. S may choose to exclude both nodes from future packet transmissions, or alternatively, apply a more extensive investigation to refine its detection. The above detection process applies to one end-to-end path. The detection for multiple paths can be performed as multiple independent detections, one for each path.

III. PROPOSED APPROACH

In this proposed work, we are going to introduce one new concept for monitoring the all the nodes from the network and getting feedback about the network from the nodes. By using this methods the all the nodes details will be gathered by all the nodes in the network. So anyone of the node is malicious node if its drops your data, based on these above information it will identify about malicious nodes. This is the task will performed repeatedly so if any one of the malicious node enters in the network it can easily identifies the malicious node. This paper proposes a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole attacks in MANETs. In this method we uses the fake request before transmitting the data to the network. The normal nodes will not reply for this fake request but the malicious node will reply for that request. So based on that reply we can easily identify the malicious node. Here after, any request from the malicious node will not be accepted by any In this case, a malicious node (so-called black hole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that “fake” shortest route to the destination and then discard these packets without forwarding them to the destination. In gray hole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a black hole attack. To resolve this issue, the function of HELLO message is added to the help each node in identifying which nodes are their adjacent nodes within one hop. We study the end-to-end delay of the CBDS and DSR for different thresholds. We have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative black hole attacks. Our simulation results revealed that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. Thus, the end-to-end delay of the CBDS for different thresholds does not increase when the number of malicious nodes increases. Although a threshold of 85% produces the shortest delay, the resulting packet delivery ratio appears to be lower than that produced threshold is set to 95% or is set to the dynamic threshold value.

IV. SIMULATION AND RESULTS

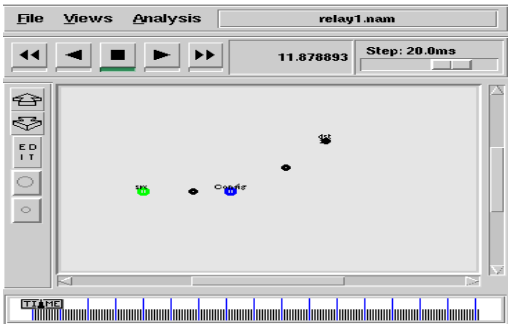

Fig. 1 Secure key transmission at all nodes

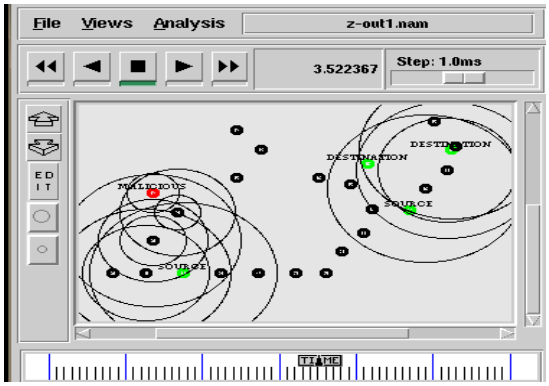

Fig. 2 Path selection and Identification of malicious node

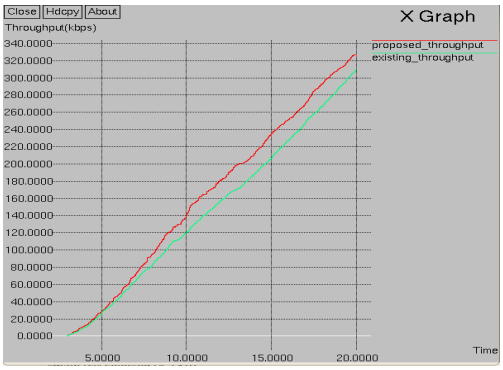

Fig. 1 Throughput (%)

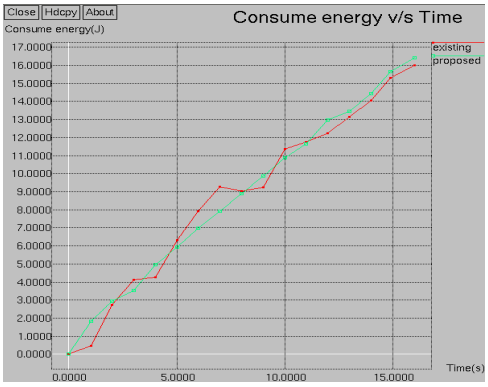

Fig. 4 Consume energy

V. CONCLUSION

In this paper, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative black hole attacks. Our simulation results revealed that the CBDS out performs the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing ovrhead and packet delivery ratio. Integration of the CBDS with other well-known message security schemes is investigated in order to construct comprehensive secure routing framework to protect MANETs against miscreants.

REFERENCES

[1] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Considerations,Jan. 1999.
[2] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. IEEE Network, 13(6):24–30, 1999.
[3] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile

ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 3064 –3073, Sept. 2011.

[4] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*,vol. 1, no. 22, pp. 28–32, 2010.

[5] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Networks*, vol. 15, no. 3, pp. 279–294, Mar. 2009.

[6] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

[7] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems*, (Bologna, Italy), Nov. 2004.

[8] H. Ma, J. Zhu, and S. Roy, "On loss differentiation for csma-based dense wireless network," Communications Letters, IEEE, vol. 11, no. 11, pp.877–879, November 2007.

[9] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers.Commun.*, vol. 29, pp. 367–388, 2004.

[10] W. Zhang, R. Rao, G. Cao, and G. Kesidis, "Secure routing in ad hoc networks and a related intrusion detection problem," Military Communications Conference, 2003. MILCOM 2003. IEEE, vol. 2, pp. 735–740 Vol.2, Oct. 2003.

[11] S. Radosavac, A. A. Cardenas, J. S. Baras, and G. V. Moustakides,"Detecting ieee 802.11 mac layer misbehavior in ad hoc networks:Robust strategies against individual and colluding attackers," J. Comput.Secure., vol. 15, no. 1, pp. 103–128, 2007.

[12] P. Kyasanur and N. H. Vaidya. Detection and Handling of MAC Layer Misbehavior in Wireless Networks. Technical report, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, August 2002.

[13] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service(QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J.Wireless Commun. Networking*, vol. 2013, pp. 188–190, July 2013.

[14] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop on SASN'05*, (Alexandria, VA,USA), Nov. 2005.

[15] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, 2006.