An Efficient Routing Method to Counter Against the Packet Dropping Attacks in MANETS

C. Visvesvaran
P.G Scholar (Communication Systems)
SNS College ot Technology, Coimbatore, India

***Abstract*— Mobile ad hoc networks (MANETs) have tremendous advantages over regular wireless networks. In MANETs, nodes usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments, some nodes may do so, either for saving their own resources or for intentionally disrupting their regular communications. This type of misbehavior is generally referred to as packet dropping attack or black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse. The special network characteristics, such as limited battery power and mobility, make the prevention techniques based on cryptographic primitives that are ineffective to cope with such attack. Rather, a more proactive method is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails, some economic-based approaches can be adopted to alleviate the attack consequences by motivating the nodes cooperation. As a backup, detection and reaction schemes remain as the final defense line to identify the misbehaving nodes and punish them. Here, we examine the challenges that remain to be tackled by researchers for constructing an in-depth defense against such a complicated attack.**

Keywords—Ad Hoc Networks, Routing Protocols Security, Packet Dropping Attack, Black Hole Attack.

I.INTRODUCTION

Mobile ad hoc networks (MANETs) are usually formed by a group of mobile nodes, interconnected via wireless links, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. That means, if a node claims it can reach another node by a certain path or distance, the claim is trusted/true; similarly, if a node reports a link break, the link will no longer be used. While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces a vulnerability to several types of denial of service (DoS) attacks particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it. Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in MANETs. A foe can easily join the network and compromise a legitimate node then subsequently start dropping packets that are expected to be relayed in order to disrupt the regular communications. Consequently, all the routes passing through this node fail to establish a correct routing path between the source and destination nodes.

Although upper layer acknowledgment, such as TCP ACK (Transmission Control Protocol ACKnowledgment) can detect end-to-end communication break, it is unable to identify accurately the node which contributes to that. Moreover, such mechanism is unavailable in connectionless transport layer protocols like UDP (User Datagram Protocol). Therefore, securing the basic operation of the network becomes one of the primary concerns in hostile environments in the presence of packets droppers. The challenge lies in securing communication meanwhile maintaining connectivity between nodes despite of the attacks launched by the foes and the frequently changing topology. It is thus obvious that both phases of the communication, mainly route discovery and data transmission phase, should be protected, calling for comprehensive security studies. While a number of surveys dealing with security threats against routing protocols in MANETs, have provided some insightful overviews on different threats and countermeasures, none of them focuses on a specific attack and examines all its characteristics in different routing techniques. To complement those efforts, this work studies the packet dropping attack, which is known as one of the most destructive threats in MANETs, and illustrates in depth the different schemes used by adversaries targeting on both reactive and proactive protocols. Furthermore, we conduct an up-to-date survey of the most valuable contributions aiming to avoid the packet droppers. The careful examination and analysis has allowed us to carry out a comparative study of the existing security schemes in terms of specific design rationale and objectives. The ultimate goal is to identify the strengths and weaknesses of each scheme in order to devise a more effective and practical solution which can achieve a better trade-off between security and network performance. The remainder of the survey is structured as follows.

In next section, we discuss the root causes of dropping packets in MANETs. Section 3 describes the Black hole attack in both reactive and proactive routing protocols. An overview of the proposed security schemes for defending against this attack and some open challenges related to the herein presented attack and solutions are highlighted. Finally,

section 4 concludes the survey and points out future research directions.

II. RELATED WORKS

A. ATTACK MODELS:

1) PACKET DROPPING IN MANETS

Before analyzing the packet dropping attack in details, let us first summarize the different motives that incite some nodes to drop a packet rather than sending or relaying it. In general, a packet can be dropped at either MAC or network layers due to the following reasons:

1. The size of packets' transmission buffer at MAC level is limited; therefore whenever the buffer is full any new packet arriving from higher layers will be dropped (buffer overflow).
2. IEEE 802.11 protocol's [4] rules: a data packet is dropped if its retransmission attempts or the one of its corresponding RTS (Request To Send) frame has reached the maximum allowed number, owing to node's movement or collision (a lot of contending nodes).
3. A data packet may be dropped or lost if it is corrupted during transmission due to some phenomenon specific to radio transmissions such as interference, hidden nodes and high bit error rate.

2) BLACK HOLE ATTACK IN MANETS

The black hole attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack. In particular the malicious node can intentionally drop all the forwarded packets going through it (black hole), or it can selectively drop the packets originated from or destined to certain nodes that it dislikes. In order to launch a black hole attack, the first step for a malicious node is to find a way that allows it to get involved in the routing/forwarding path of data/control packets.

To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network. Thus in fig.1 any node can easily misbehave and provoke a severe harm to the network by targeting both data and control packets. Dropping data packets leads to suspend the ongoing communication between the source and the destination node. More seriously, an attacker capturing the incoming control packets can prevent the associated nodes from establishing routes between them. To facilitate understanding, we illustrate them using representative routing protocol in MANETs.

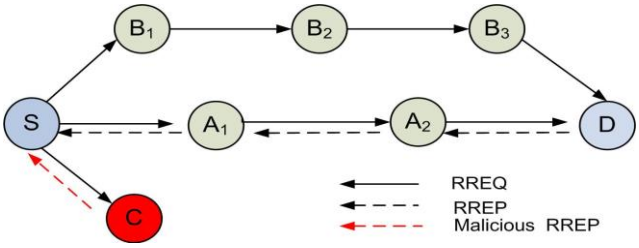

Fig 1: Black hole Attack in MANET

3) DSR protocol

Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by[6]. In a nutshell, it works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it and sends mess ages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link. Since DSR has no security mechanism they are vulnerable to much type of attacks. It assumes all nodes cooperate in the network so in its present status cannot defend itself from attacks.

III. SECURE MANETS AGAINST BLACK HOLE ATTACK

Recently, many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability. In what follows, we give a snapshot of the mostly used cryptographic primitives in MANETs.

A. *Overview of the cryptographic primitives*

As MANETs become more ubiquitous, the need for providing adequate security tools gets to be more obvious. The existing security schemes in such networks use generally one or more of the following cryptographic technologies: symmetric-key cryptography [15], digital signature [3], threshold cryptography [1] and one way hash chain [2]. Each of these cryptographic primitives has its specific advantages and drawbacks. For example, the security schemes based on digital signature and threshold cryptography generate much more computational overhead than those based on symmetric cryptography. However, the security approaches that are solely based on symmetric-key cryptography are less robust and offer less security than asymmetric key cryptography, due to the higher probability that the shared keys being compromised. As one way chains are known to be very efficient for verification, they became increasingly popular for designing security protocols for hand-held devices. This is due to the fact that the low powered processors are able to compute a one way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature [8], Consequently, recent wireless ad hoc network's security protocols extensively use one way chains to design protocols that scale down to resources constrained devices. These cryptographic schemes are known to be efficient to ensure several properties such as confidentiality, data integrity and non repudiation. However, they cannot be adopted in MANETs since a Certificate Authority (CA) or a Key Distribution Center (KDC) is not always available. Moreover, these techniques cannot prevent a malicious node from dropping packets supposed to be relayed, which is our focus in this survey.

B. *Reputation based schemes*

The reputation is the art of using historic observation about the behavior of a node to determine whether it is trustworthy or not. Each node must form an opinion regarding the other nodes based on their observed past behaviors. Then the nodes with low reputation are punished or avoided while establishing routes. The major drawback of this category is the excessive traffic exchange needed for sharing the reputation information between the nodes. Moreover, a serious vulnerability of reputation based schemes is the fact that any compromised node can send forged reputation information in order to decrease the trust level of some nodes. In what follows, we describe three representative schemes that use the reputation mechanism.

C. *Cross-layer cooperation based schemes*

Most of the existing solutions rely on the Watchdog technique to ensure the correct forwarding of packets by the neighboring nodes; however this technique suffers from certain Weaknesses, particularly when power control is applied. In a low cost approach dubbed (SMDP) to circumvent the aforementioned drawbacks of Watchdog. They have designed a cross layer scheme that ensures higher detection accuracy. In this scheme, it is required that the routing protocol be aware of the beginning and end of each continuous traffic routed through it. This can be accomplished through cross-layer cooperation between network and session layers.

At the end of each session, every node involved in the forwarding path sends out two signed packets, one to each successor node containing the number of packets sent to it, and the other packet towards its predecessor node contains the number of packets received from it. According to the received packets, each node broadcasts to its one hop neighbors a special packet called Forwarding Approval Packet (FPA) as a proof of its cooperation. On receiving this packet the neighbors of the sender can judge whether this node has correctly forwarded the packets or not. The main advantage of this scheme is its high detection accuracy that significantly reduces the number of false alarms.

IV. CONCLUSION

In this survey we have presented a survey of the state of the art on securing MANETs against packet dropping attack. The attack schemes, as well as prevention, detection and reaction mechanisms have been explored. We categorized them into three categories according to their goals and their specific strategies. A comparative study between them was then conducted to highlight their respective effectiveness and limitations. We concluded that most of the proposed schemes in the first, second or third defense line are based upon certain assumptions that are not always valid due to the dynamic nature of MANETs and their specific characteristics. Many researchers have been motivated to apply game theory to enforce nodes cooperation in MANETs, such as the works done. These works assume that a node tries always to maximize its benefit by choosing whether to cooperate in the network or not. However, those works are generally based on the assumption that the majority of the nodes are misbehaving, which is not an usual case in MANETs. We believe it is an interesting and significant topic for further exploration with more realistic assumptions, especially tailored for packet dropping attack.

V. REFERENCES

[1] A. Shamir, How to Share a Secret, *Communications of the ACM*, 22(11): 612-613,November 1979.
[2] L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM*, 24(11): 770-772, November 1981.
[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, *CRC Press*, October 1996.
[4] IEEE 802.11 wireless LAN media access control (MAC) and physical layer (PHY) specifications, ANSI/IEEE Std 802.11, 1999.
[5] D. B. Johnson and D. A. Maltz, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft), Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.
[6] S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating routing misbehaviour in mobile ad hoc networks, *In Proc. 6th annual international conference on Mobile computing and networking (MOBICOM '00)*, Boston, Massachusetts, USA, August 2000.
[7] B. Schneider, Secrets and Lies. Digital Security in a Networked World, John Wiley & Sons, inc, 1*st* edition, 2000.
[8] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes, PGP in constrained wireless devices, *In Proc. 9th USENIX Security Symposium*, Denver, Colorado, August 2000.
[9] L. Buttyan and J. P. Hubaux, Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Mobile Ad Hoc Networks,

Swiss Federal Institution of Technology, Lausanne, Switzerland, Tech. Rep. DSC/2001/001, January 2001.

[10] S. Buchegger and J. Y. Le Boudec, Performance Analysis of the CONFIDANT Protocol, *In Proc.* 3*rd ACM International Symposium on Mobile Ad Hoc Networking & computing (MOBIHOC'02)*, Lausanne, Switzerland, June 2002.

[11] Y. C. Hu, A. Perrig and D. B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks, *In Proc.* 8*th ACM International Conference on Mobile Computing and Networking*, Westin Peachtree Plaza, Atlanta, Georgia, USA, September 2002.

[12] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless ad hoc networks, *IEEE Commun. Mag.*, 40(10): 70-75, October 2002.

[13] B. Sun, Y. Guan, J. Chen and U. W. Pooch, Detecting black- hole attack in mobile ad hoc networks, *In Proc.* 5*th sEuropean Personal Mobile Communications Conference*, Glasgow, UK, April 2003.

[14] C. Perkins, E. Belding-Royer and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, *IETF RFC 3561 (Experimental)*, July2003.