Journal of Network and Computer Applications 80 (2017) 189–199

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

# HSecGR: Highly Secure Geographic Routing

Mehdi Boulaiche*, Louiza Bouallouche-Medjkoune

*LAMOS University of Bejaia, Algeria*

ARTICLE INFO

*Keywords:*
Ad hoc network
Secure routing
Attack
Cryptography
Reputation
Malicious

ABSTRACT

An ad hoc wireless network is a set of nodes connected by wireless links in which nodes cooperate to forward packets from a source to a destination. Geographic routing (or position-based routing) has become an attractive solution for such networks since it reduces routing control overhead flooded in the network to construct routes (routes discovery). Many geographic routing protocols have been designed to guarantee packet delivery in such networks. However, these protocols consider that all nodes in the network are trustworthy which allows malicious nodes to violate network security and disrupt packet forwarding. In this paper, we propose and evaluate a new security approach that secures geographic routing protocols against a variety of attacks. Our approach is based on the use of MACs to allow intermediate nodes to verify the authenticity and the integrity of forwarded packets and uses authenticated acknowledgements to prevent packet dropping attacks. To meet node's resource constraints, we have based our solution on symmetric cryptography. Our solution is robust against modification and dropping attacks even in the presence of compromised nodes in the network.

## 1. Introduction

An ad hoc wireless network is a set of nodes connected by wireless links where all nodes in the network cooperate to forward packets from one point to another. The protocols designed for routing in this type of networks are different from those designed for routing in wired networks. Routing protocols designed for wireless ad hoc networks have to deal with the characteristics of such networks. These protocols have to be designed so as to minimize communication overhead since nodes have limited resources. They also need to handle mobility of nodes within the network. And very importantly, a routing protocol designed for such networks should mitigate the impact of attacks on the protocol. Indeed, due to the broadcast nature of wireless channel it is sufficient that an attacker be in the transmission range of a node to eavesdrop on the on-going traffic, tamper, or drop packets since every node in the network is expected to participate in packet forwarding process.

There are three main categories of routing protocols for ad hoc wireless networks namely: flat routing, hierarchical routing, and geographic routing. Flat routing protocols include reactive protocols such as DSR (Boukerche et al., 2011), AODV (Mulert et al., 2012) and proactive protocols such as DSDV (Ade and Tijare, 2010). In hierarchical routing, nodes are divided into clusters and a cluster head is assigned to each cluster head. LEACH (Tyagi and Kumar, 2013) is an example of hierarchical routing protocols. In geographic routing protocols, the position information of nodes is used to forward packets toward the final destination. GPSR (Karp and Kung, 2000) is an example of geographic routing protocols.

Geographic routing has become an attractive solution (Milocco et al., 2014; Peng and Kemp, 2011; Lee et al., 2010a; Boulaiche and Bouallouche-Medjkoune, 2015; Tao et al., 2010; Kleerekoper and Filer, 2015; Al-shugran et al., 2013) for wireless ad hoc networks where nodes keep only information about local one hope neighbors. In geographic routing, a node selects a next forwarding node based only on the location of itself, its neighbors and the destination. The location information can be obtained with GPS or through any other localization system. As it does not use control packets to establish a path, the geographic routing reduces routing control overhead flooded in the network to maintain network connectivity compared with other types of routing protocols. Protocols called *greedy* (Al-shugran et al., 2013) forward packets such that their routes be the closest to the path as the crow flies between the source and the destination. NFP (Al-shugran et al., 2013) protocol selects its closest neighbor among those in the direction of the destination to forward the packet. Whereas, with MFR (Al-shugran et al., 2013) protocol, a forwarding node selects its neighbor that is closest to the destination as next forwarding node. NADV (Lee et al., 2010b) selects the neighbor with the optimal trade-off between the advance and link cost. To overcome *holes* (Chen and Varshney, 2007) problem (known also as *local minima*) in geographic routing protocols, solutions proposed in (Karp and Kung, 2000; Tao et al., 2010; Won et al., 2013) use the right (or left) hand rule (Chen and Varshney, 2007) to forward packets around the *holes*.

* Corresponding author.
*E-mail addresses:* boulaiche.mehdi@yahoo.fr (M. Boulaiche), louiza_medjkoune@yahoo.fr (L. Bouallouche-Medjkoune).

http://dx.doi.org/10.1016/j.jnca.2016.12.028
Received 21 December 2015; Received in revised form 12 November 2016; Accepted 19 December 2016
Available online 25 December 2016

Geographic routing protocols forward packets based on the assumption that all nodes in the network are trustworthy and don't take into account the security problem. However, the presence of malicious (or compromised) nodes in the network, can lead to a degradation in the performances of geographic routing in terms of delivery ratio (routing failures). In geographic routing, a forwarding node selects its next hop according to the destination position contained in forwarded messages. An attacker may alter or modify this information to disrupt the routing scheme. An attacker may also generate falsified messages such as beacon messages or error messages to disrupt routing scheme. These types of attacks can be used with the *blackhole attack* (Sarma et al., 2011) in which a node drops all packets going through it, or with *sybil attack* (Md Zin et al., 2014) in which the attacker provides multiple identities to other nodes in the network. Another type of attacks that can be launched against geographic routing is *wormhole attack* (Qazi et al., 2013), two malicious nodes cooperate and build a tunnel between them and get packets from one region to another. This type of attacks is very difficult to detect.

In this paper we will propose a Highly Secure Geographic Routing approach. The objective of our work is to provide a mechanism that allows both intermediate nodes and the destination node to verify the authenticity and the integrity of forwarded packets in one hand and to protect against dropping attacks on the other hand. Our solution is based on the use of MACs (Message Authentication Code) with a secret key to protect packets against modification and to prevent attackers from tampering routing information. To protect packets against dropping attacks, each intermediate node that receives a packet must return back an authenticated acknowledgement to the packet's source indicating both the previous and the next hop for this packet. For this, we propose an extension to the packet header to provide these security services for geographic routing protocols. Our solution is robust against modification and dropping attacks even in the presence of compromised nodes in the network. To meet node's resource constraints, we have based our solution on symmetric cryptography.

The rest of the paper is organized as follows: Section 2 presents related work on secure routing protocols in ad hoc networks. Our security approach that protects against these security attacks will be presented and detailed in Section 3. Simulation results will be discussed in Section 4. Section 5 concludes this paper.

## 2. Related work

The use of wireless links significantly facilitates attacks against routing protocols in wireless ad hoc networks. Unlike wired networks where the attacker must have physical access to the network, in wireless ad hoc networks, it is sufficient that the attacker be in the transmission range of a node to eavesdrop on communications, modify, or inject packets in the network. To address routing security problem in ad hoc networks, several solutions have been proposed in the literature. Generally speaking, these solutions propose extensions to already existing protocols in order to strengthen their security efficiency against some attacks.

Authors in (Baadache and Belmehdi, 2012, 2014) proposed an approach that allows to secure both proactive and reactive routing protocols against simple and cooperative black hole attack. In (Yu et al., 2009) authors proposed SRAC a secure routing protocol to defend Byzantine attacks as well as other internal attacks against routing protocols for MANETs in adversarial environments by using both message and route redundancy during route discovery. Authors in (Zhang et al., 2014) proposed TOHIP a TOpology-HIding multipath routing Protocol which does not allow packets to carry routing information so that the malicious nodes cannot deduce network topology and launch various attacks based on that. Authors in (Djenouri and Badache, 2009) suggest a modular solution structured around five modules to monitor, detect, and safely isolate misbehaving nodes that drop packets in mobile ad hoc networks.

Other work in secure routing (such as Ade and Tijare, 2010; Perrig et al., 2005; Kim and Tsudik, 2009; Tygar et al., 2002; Buttyan et al., 2006; Yi et al., 2001; Levine et al., 2002; Zapata and Asokan, 2002; Johnson et al., 2003; Wang et al., 2010), is about protecting topology (route) discovery. ARIADNE (Perrig et al., 2005) and SRDP (Kim and Tsudik, 2009) are two protocols that provide an extension to secure route discovery in DSR (Boukerche et al., 2011) protocol using cryptographic tools. ARIADNE provides three patterns (shared secret keys between any pair of nodes, *TESLA* (Tygar et al., 2002), or digital signature) to authenticate information provided by intermediate nodes between the source and the destination. However, analysis of ARIADNE protocol in (Yi et al., 2001) has shown some security vulnerabilities in the protocol. Authors in (Buttyan et al., 2006) proposed to sign *Route Reply* field instead of signing *Route Request* to eliminate these security vulnerabilities. Authors in SRDP (Kim and Tsudik, 2009) Proposed the use of either aggregated message authentication codes (MACs) or multi-signatures to securely discover an authenticated route to the destination in DSR.

To secure AODV (Mulert et al., 2012) protocol, Authors in SAR (Yi et al., 2001) ARAN (Levine et al., 2002), S-AODV (Zapata and Asokan, 2002) propose other extensions that can provide security properties for AODV protocol. In SAR protocol, nodes in the network are divided into confidence levels. Consequently, only nodes that belong to a higher confidence level than the minimum required level can participate in route search process. S-AODV protocol proposes to use a digital signature to authenticate *non-mutable* fields of the message (fields that don't change since message creation) and use a hash chain to protect the *hop_counter* field. SEAD (Johnson et al., 2003) and SDSDV (Wang et al., 2010) are two protocols that have been proposed to provide security services for DSDV protocol (Ade and Tijare, 2010). SEAD protocol tries to protect DSDV *sequence_number* field against modification attacks using a hash chain. Whereas, SDSDV tries to improve DSDV security by preventing nodes from increasing or decreasing *distance_metric* and *sequence_number* fields.

In detective solutions, CONFIDENT (Buchegger and Le Boudec, 2005) and *Watchdog* & *Pathrater* (Kevin et al., Mary.) protocols are two protocols that have been proposed to enhance the security of DSR protocol. By monitoring nodes behavior in the network, malicious nodes are isolated in *black lists* and thus will be avoided during packet routing. TAODV (Lyu et al., 2004) is another solution that has been proposed to improve AODV security based on node behaviors in the network.

To secure geographic routing protocols, Chen L. et al. proposed in (Lyu et al., 2013) the use of geographic leashes and the TESLA scheme to provide resistance against the Sybil attack and wormhole attack and the use of a distributed trust model and the packets opportunistic forwarding to prevent black hole and gray hole attacks. In (Marin-Perez and Ruiz, 2011) Rafael M. et al. proposed a Self-Protected Beaconless Geographic Routing protocol (SBGR) in which nodes overhear the forwarding of their neighbors to detect malicious behaviors. Authors in (Pathak et al., 2008) proposed GSPR an infrastructure free geographic routing protocol that is resilient to disruptions caused by malicious or faulty nodes. Authors in (Song et al., 2007) proposed secure geographic forwarding (SGF) that incorporates both the Hashed MAC and the TESLA to provide security mechanisms for both data and control messages in geographic routing protocols.

Most of the earlier works deal with only one type of attacks but not with a variety of attacks that can be launched against a routing protocol. For example, solutions proposed in (Perrig et al., 2005; Kim and Tsudik, 2009; Tygar et al., 2002; Buttyan et al., 2006; Yi et al., 2001; Levine et al., 2002; Zapata and Asokan, 2002; Johnson et al., 2003; Wang et al., 2010) protect route discovery packets against modification attacks. However, these solutions don't protect against packet dropping attacks. Contrary, solutions proposed in (Buchegger and Le Boudec, 2005; Kevin et al., 2000; Lyu et al., 2004) protect against packet dropping attacks but don't protect against modification