Chapter 15
Trust-Based SAODV Protocol with Intrusion Detection, Trust Management and Incentive Cooperation in MANETs

Floriano De Rango
DEIS Department, University of Calabria, Rende (CS), Italy

ABSTRACT

Distributed wireless systems present many security issues, and offering security preserving network resources is often a challenging effort. Offering security through only cryptography is not always a suitable solution if the high dynamic context of MANET is considered and the trust mechanism that reduces the computationally intensive number of security operations becomes strategic. In this work, a well-known routing protocol, called SAODV, has been considered. To improve its performance and offer more resilience to attack from malicious nodes authenticated by the network, some additional features are added. A preventive approach based on a cryptographic mechanism and a reactive approach to detect anomalous and malicious nodes are considered. An extension of SAODV offering an Intrusion Detection Mechanism (IDM) and a Trust-based Mechanism (TBM) to promote the collaboration of the cooperating nodes and penalize the selfish nodes are proposed. Simulation results were performed under a NS-2 simulator to show the effectiveness of our proposal compared with AODV and SAODV. Simulation parameters, such as Normalized Routing Overhead, Data Packet Delivery Ratio, average number of signatures and throughput of collaborating and malicious nodes, have been considered.

INTRODUCTION

In MANET the security issue is a hot and challenging task, considering the distributed nature of the communication and the absence of any underlying fixed infrastructure (Royer & Toh, 1999). Mobile host join on the fly and create a network on their own. With the network topology changing dynamically and the lack of any centralized network management functionality, these networks tend to be vulnerable to a number of attacks. These attacks can be assessed by node external to the networks or by node already authenticated in the network (internal attacks). This means that...
for this kind of network a distributed monitoring system to verify the actions of mobile nodes and a signature mechanism to verify the identity and authenticity of nodes become necessary. However, it is important to observe that any security mechanism introduced in the node features need to be scalable and not too complex due to the limited resources of mobile nodes. In literature there are many routing protocols for MANET that offer some security features (Wu, Chen, Wu, & Cardei, 2006). However, these protocols consider just some specific aspects of security. In this case, we tried to consider more features like intrusion detection, trust establishment among nodes and incentive cooperation to reduce the selfish behavior that can reduce the network performance. In order to reduce the computational complexity of mobile nodes, only a preventive mechanism such as cryptography can be unsuitable. In this last case, Intrusion Detection Mechanism (IDM) and Trust-based Mechanisms (TBM) can become essential (Anantavalee & Wu, 2006; Pirzada, McDonald, & Datta, 2006). To combat malicious behavior coming of nodes authenticated by the network, reactive approaches based on the observation node activity can become important and appealing. Often, both approaches (IDM and TBM) can request a supplementary deployment of resources and an additional overhead not present in the traditional routing protocols (Anantavalee & Wu, 2006; Pirzada et al. 2006). Owing to this overhead, both of them are always considered separately. However, we think that through a joint and efficient use of both solutions, a greater degree of security can be offered for the right working of a routing protocol in a MANET.

Our proposal will reduce the complexity of signature mechanism the hop counting procedure from source and destination in the route discovery process. Moreover, a trust management based on trust levels will be proposed. Through this approach it will possible to associate different security actions. Additionally to this feature, also a collaboration grade index is defined in order to promote the cooperation among nodes and to individuate selfish nodes in the network. In our proposal, selfish behavior is discouraged through penalty actions.

The paper structure will be the following: some related works on security protocols, Intrusion Detection mechanisms and Trust Management over MANETs are presented in the next section; the SAODV protocol will be examined in another section (Zapata, 2006); later the additional security features introduced in SAODV and trust-level management are presented; finally, simulations results and conclusions are respectively presented.

RELATED WORK

In the literature many attacks (Wu et al., 2006) have been actuated in a MANET to produce Denial of Service (DoS). Regarding on-demand protocols, the route discovery phase can be a weak point of the protocol. For example, during the RREQ propagation a node can modify some fields of the packet in order to determine the selection of the path that goes through itself. In this section we briefly refer to some well-known secure routing protocol and then the attention will be focused on the Intrusion Detection Mechanism proposed in literature and the Trust Management policies.

Security-Based Protocols

Protocols that make use of the public key cryptography to generate signature, or protocols that use symmetric cryptography or hash functions are proposed (Perrig, Johnson, & Hu, 2004).

The first routing solutions are represented by protocols such as SAODV (Zapata, 2006), which will be discussed in the next section, SRP (Papadimitratos & Haas, 2002) that represents an extension of the protocol DSR for some security mechanism support, SEAD (Hu, Johnson, & Perrig, 2002a) and Ariadne (Hu, Johnson, & Perrig 2002b) that introduce a security mecha-