RESEARCH ARTICLE OPEN ACCESS

Review of MANET Utilization for Watermarking Algorithms

Mohamad T. Sultan*, Khaled N. Yasen **
**(Department of Computer Science, Faculty of Science, Cihan University-Erbil, Erbil, Iraq*
*** (*(Department of Computer Science, Faculty of Science, Cihan University-Erbil, Erbil, Iraq*
*Corresponding Author : Mohamad T. Sultan**

ABSTRACT
Wireless communications are being used in a wide range of environments and evolved in many applications. Mobile Ad hoc networks as one of wireless technologies has the flexibility for nodes to join and leave the network frequently at any time. However, this flexibility came with set of issues in security as forgery, fabricated routes and many others. In this paper a review of the utilization of watermarking system as an authentication protection and security tool in MANET is presented to conclude future requirements of watermarking in MANET security.

Keywords: MANET; Wireless Networks; Security; Watermarking.

Date of Submission: 07-11-2017 Date of acceptance: 25-11-2017

I. INTRODUCTION

Recently, mobile ad-hoc networks MANETs are extensively used in a wide applications in different fields [1]. Mobile ad-hoc network has been used in different applications networks range [2] from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time which makes it vulnerable to various security and provide ways for attacks to get into the network and thus suspects the security. So, there arises a great need to provide more secure solutions to MANET as compared to traditional wireless network [3]. Many solutions have been proposed in recent researches for secure routing protocol to increase the security of MANETs. [4]. One of these solutions is the usage of watermarking schemes, watermarking is the process of embedded a hidden piece of data inside the host work, the information may be used as metadata, proof of ownership or any information that might be needed to be embedded by author [5]. Cryptography along with watermarking are both tackle the issue of computer security, but watermarking have additional uses other than securing applications. For multimedia and network security such as wireless MANETs issues are typically handled through cryptography; however, cryptography only ensures confidentiality and authenticity when a message is transmitted through a public channel such as an open network or wireless node in MANETs, but it can be detected by malicious attacks, which can observe or intercept a transmission channel. Because there is a change in the structure of the data unreadable it can arouse suspicion and curiosity. Moreover, digital watermarking differs from cryptography, because it leaves the original medium or data almost entirely unaltered, thus it is an effective way to protect secure data to multimedia data even after its transmission then, digital watermarking solutions can be used to prevent the impact of active or passive attacks and which provide evidence of its authenticity[2]

The digital watermarking solutions can be employed to prevent the impact of external attackers of MANET by mutual authentication of the participating nodes through authenticated digital watermarking in spatial domain scheme.

In this paper, a review of current attempts in securing MANET systems with watermarking is presented, as securing the routing algorithms, ensure the availability of communication in spite of adversary nodes, intrusion detection..etc. with an analysis of future requirements in employing cryptographic algorithms in MANET. Next section lists security issues in MANET. Section three is about watermarking attempts in MANET, while section four presents a brief analysis of some watermarking featured that still not utilized in MANET. A conclusion is presented in section five.

II. SECURITY ISSUES AND ATTACKS

Although MANET present many advantages, they also present a number of inherent vulnerabilities that increase their security risks

[10][11]. MANET are often subject to eavesdropping, signal jamming and other types of attacks, due to the open medium, the dynamically changing topology, the lack of a centralized monitoring and management point, the limited resources and the lack of physical security of the member nodes.

Special characteristics in MANET's as dynamic topologies and frequent connecting and disconnecting of nodes cause a set of security issues as [6]:

- everyone, which make the network prone to intruders.
- Adversaries can easily join and become part of the network.
- There are no specific infrastructure for dividing and addressing nodes, authentication, etc.
- Mobile nodes mostly have limited capabilities, their availability can easily be compromised
- Cooperation based security algorithms must consider the bandwidth limitation associated with links

As the nodes are dependent on each other for routing, adversaries can generate fabricated routes to wrongly forward packets.

In addition to security gaps, general attacks as an active attack and Passive attack as shown in Fig. 1 also should be considered, an active Attack is a type of attack where an attacker gets access to the medium of communication and modifies or disrupts the transmission. For example, Denial of Service (DoS) attack attempts to overwhelm a target machine (via sending huge number of communication requests), so that the victim can't respond to legitimate requests of other hosts.

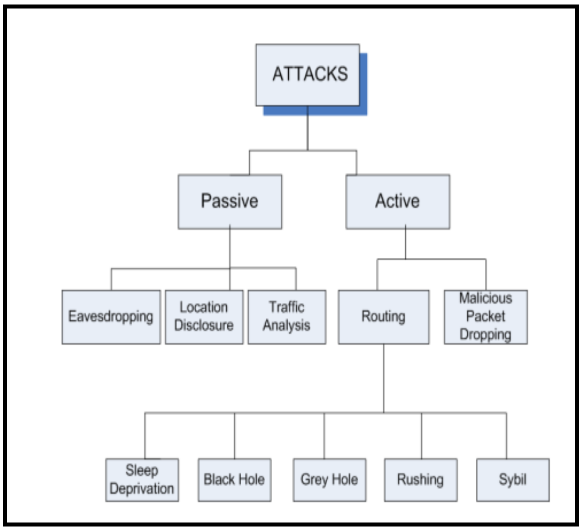

Figure 1: Classification of attacks in MANETs

A passive attack only observes the ongoing transmission but doesn't alter or disrupts any activity. A common example is traffic analysis of the snooped data to discover passwords and confidential information of other users. Active attacks usually target integrity and availability of system while passive attack tries to break the confidentiality of the security system [6].

III. WATERMARKING ATTEMPTS IN MANET

Watermarking is the method for protecting the related data that should exchange between nodes, or is imperceptible added to the cover-signal in order to convey the hidden data. Watermarking techniques are then applied in order to prevent the possible modification of the produced maps.

One of the first attempts in utilizing watermarking schemes in MANET was by Mitrokotsa et.al in 2007, when they presented an authenticating way for local and global maps using watermarking in order to prevent the possible modification of produced maps. Proposed method derives from the combination of two watermarking embedding methods, the Lattice and the Block-Wise. The proposed combined watermarking method exploits the advantages of the Lattice and the Block-Wise method in order to produce the most efficient and reliable results [7]. The Lattice and the Block-Wise are utilized again by same authors in 2010 [8] by employing them with a type of neural network model called eSOM (emergent Self-Organizing Maps) for an intrusion detection approaches, when most sensitive part of the eSOM map that represents the existence of an attack in a node being the most sensitive part of the map is watermarked with the Block-Wise method and the rest of the map with the Lattice embed-ding method. Different quality metrics had been utilize in this work to measure the difference between original and watermarked work, as Normalized Cross Correlation (NCC) and Peak Signal to Noise Ratio (PSNR). In proposed algorithm, each node of the MANET should perform its local intrusion detection using local audit data.

In 2011 Aliwa et.al proposed an authenticated digital watermarking algorithm in mobile ad-hoc distance vector routing protocol (AWDV) to provides a secure routing protocol and compared with two ad-hoc routing protocols such as SEAD secure routing protocol and traditional DSDV routing protocol. authenticated digital watermarking algorithm in mobile ad-hoc network is done by modifying the destination sequenced distance vector routing protocol DSDV used to embed watermark bits in each authentic routing advertisements to create authentic watermarked packet entry in an routing update, whereas the mobile nodes maintain an additional table with new table entry of authentic route (AWDV)[4].

Another attempt by Aliwa is was in 2014 [2], by developing a scheme for improving security of AWDV routing protocol. It is used to embed a watermark as an authentication and hide the owner address of source node as an evidence and number of hops to reach the destination node, in order to create authentic "watermarked packet" entry at each authentic route update, whereas the mobile nodes maintain an additional table with a new table entry of authenticated route.

IV. ANALYSIS

The goal of mobile ad-hoc security is to safeguard the nodes' operation and ensure the availability of communication in spite of adversary nodes. [2]. by comparing the extensive usage of watermarking systems in computer fields and specifically in network, one realize that the usage of such algorithms in MANET is in early stages. i.e, watermarking methods are not completely utilized in MANET yet. For example, transform domain watermarking which used to produce better results in robust watermarking and its usage for copyright protection while embedding the watermark in approximate bands, or the usage of fragile and semi fragile watermarks in high frequency bands still not employed in MANET, also, packet tracking that are used in broadcasting can also be used to keep record of packet forwarding using watermarking. In addition to the ability to assesses the QoS (quality of services) of the multimedia services and dual purpose watermarking systems as presented in [9].

V. CONCLUSION

MANETs is a collection of nodes that they are randomly placed in operational environment without any before defined structure. The literature of the usage of mobile ad-hoc networks MANETs for watermarking algorithms came with a lot of advantages as increasing the routing security in presence of malicious nodes and intrusion detection, by the combination of watermarking with current MANET algorithms and routing protocols. However, full exploiting of MANET for watermarking abilities and features is not presented yet. For future work, we aim to propose intrusion detection and watermarking algorithm which can be employed to various routing protocols and used for the detection of numerous kinds of attacks as well as test it in real MANET applications and wireless ad hoc networks.

REFERENCES

[1] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE communications surveys & tutorials, 15(4), 2027-2045.

[2] Aliwa, M. B. (2014). Secure Authentication Watermarking in Ad-hoc Destination-Sequenced Distance-Vector Routing Protocol. International Journal of Computer Science and Network Security (IJCSNS), 14(5), 26.

[3] Ahuja, L., & Gupta, K. SECURITY ALGORITHMS IN MANET.

[4] Aliwa, M. B., El-Tobely, T. E. A., Fahmy, M. M., Nasr, M. E. S., & El-Aziz, M. H. A. (2011). A Novel Authenticated Digital Watermarking in Mobile Ad A Novel Authenticated Digital Watermarking in Mobile Ad-hoc Networks Using Networks Using ns-2 Simulator. IJCSNS, 11(4), 44.

[5] Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). Digital watermarking and steganography. Morgan Kaufmann.

[6] Islam, N., & Shaikh, Z. A. (2013). Security issues in mobile ad hoc network. In Wireless Networks and Security (pp. 49-80). Springer Berlin Heidelberg.

[7] Mitrokotsa, A., Komninos, N., & Douligeris, C. (2007, July). Intrusion detection with neural networks and watermarking techniques for MANET. In IEEE International Conference on Pervasive Services (pp. 118-127). IEEE.

[8] Mitrokotsa, A., Komninos, N., & Douligeris, C. (2010). Protection of an intrusion detection engine with watermarking in ad hoc networks. International Journal of Network Security, 10, 93-106.

[9] Maity, S. P., Kundu, M. K., & Maity, S. (2009). Dual purpose FWT domain spread spectrum image watermarking in real time. Computers & Electrical Engineering, 35(2), 415-433.

[10] Makki, S., Pissinou, N., & Huang, H. (2004). The Security Issues in the Ad-Hoc on Demand Distance Vector Routing Protocol (AODV). In Security and Management (p. 427).

[11] Komninos, N., Vergados, D., & Douligeris, C. (2007). Detecting unauthorized and compromised nodes in mobile ad hoc networks. Ad Hoc Networks, 5(3), 289-298.