Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 3, June 2021: 2439-2447

Research Article

A SURVEY ON SECURITY ISSUES OF FITNESS FUNCTION IN MOBILE AD HOC NETWORK

Y.Kingston Albert Dhas[1] Dr. S. Jerine[2]

ABSTRACT

It is difficult to ensure the security of mobile ad-hoc networks, particularly because wireless networking is unstable, node security is limited, topology is changing dynamically, licensed bodies are absent and there is no central surveillance and control center. In previous MANET enquirers, protocols were established to address a number of fundamental questions such as routing and the formation of new networks. However, all nodes are protected and do not take the protection factor into account. They are also subject to have deviation from what is expected. More recent research has centered on MANET security problems and potential protocol and application frameworks. This paper dealt with these inquiries. It also addresses many security problems and solutions on the various network layers currently being proposed by MANET. This article addresses topics related to security such as routing, data transfer, media access, key management and IDS. A safety survey for the MANET is available in this survey.

Keywords: MANET, Security issues, Routing Protocols

INTRODUCTION

The ongoing development of wireless devices such as laptops, PDAs, cables and wireless sensors demonstrated the skills and value of nomadic computing and mobile ad hoc networks in particular. In some mobile apps, reliance on fixed networks cannot be preserved.

[1]Research Scholar., Department of Computer ScienceNoorul Islam Centre For Higher Education
[2]Associate Professor,Department of Software Engineering Noorul Islam Centre For Higher Education

For example, disaster relief in a dam of flood and earthquake, digital human sensors in a region, military tanks and aviation's in the war, and finally knowledge sharing in a lecture (or

conference) by students (or researchers). This wish for networking independence leads to a new mobile network called ad hoc networking. We talk about this. MANET is the interim network of mobile hosts, which create dynamic in-air networks without central administration. The functions of a strong fixed infrastructure within conventional networks must be assured by mobile hosts used in MANET. This is a hard job, as resources (CPU, storage, power etc.) are limited. In addition, the network environment provides many features, such as periodic shifts in topology and bandwidth limitations for wireless networks. Previous ad hoc network research finding solutions to certain key issues in order to address emerging problems in the abovementioned areas. However, these solutions must be safe and scalable to make the device operate properly and tolerable to service quality in a fragile environment. Recent research on safety issues was focused on MANET, and methodologies and approaches were suggested for securing key protocols and applications. We discuss various security issues in MANETs in various network layers in this paper. The remainder of the article is structured accordingly. We also initially implemented some fundamental concepts, followed by security issues with routing protocols and data transfer on the same (network) layer. We are also concerned about MAC layer protection problems. The key management is introduced along with MANETs' intrusion detection systems, a clear and necessary mechanism for safe use and the underlying protocols. The key management is then implemented. We concentrate on a changing ad-hoc form of networking, i.e. sensor networks. Many security concerns are posed in this particular application.

ANALYSIS OF BASIC PARAMETERS OF SECURITY ISSUES IN MOBILE AD HOC NETWORK

Ad-hoc network security systems are not completely unlike others. In order to deter attacks and abuse, the aim of these services is to protect information and resources.We clarify the following requirements when dealing with network security that an efficient architecture of security can ensure:

Disposal: Ensure that the network service needed is available in the midst of attacks, where possible. MANET systems are designed to combat service denial and hunger and node error attacks including egoism for node-sharing packets. All of these threats will be posed later on by systems which guarantee access to MANETs.

Authentication: Ensures real matching of nodes. In other words, a trustworthy network node should not be disguised as a malicious node.

Confidentiality of data: Ensures that no other person except the intended recipient cannot access a message. In general, for use of symmetrical and asymmetrical data encryption, data confidentiality is required.

Integrity: Means the trust of node to node data. It also guarantees that node A to node B was not moved to C. It is just as simple to ensure data integrity before encrypting messages when solid privacy safeguards are implemented as by using one-way hash [1]. Non-repudiation: The power of computer networks ensures that the node does not ignore its post. There is a stable digital signature [1].

MANET AND ITS SECURITY IMPACT

By using wireless communications, ad hoc networks are susceptible to wireless attacks. Wireless, ad-hoc network attacks can occur in all directions and target any node instead of cable networks where opponents have physical access to network cables or pass through various firewall and gate protection lines. There is no simple defensive line for ad-hoc networks and each node needs to be prepared to withstand attacks. Additionally, MAC protocols such as IEEE 802.11 are used to ensure high risk channel access through safe neighborhood coordination.

Multi-hop: Hosts are their own routers and central routers or portals are not available. So packets travel multi-hop routes and travel through mobile nodes before reaching your ultimate destination. The potential lack of reliability of nodes implies a significantly poor function.

Node movement autonomy: Mobile nodes are typically autonomous, separately roaming machines. This means that it is not easy to track a single mobile node in the big ad hoc network.

Amorphous: Mobility node and wireless communications make it possible for nodes to link and leave the network by chance. Network tops therefore have no fixed form, i.e. they constantly vary in size and form. This functionality must be considered for any safety approach.
Power limitations: Small and lightweight mobile ad hoc hosts also provide low-energy energy with small batteries. This restriction results in a weakness in which attackers can target batteries that can cause a network partition to be disconnected. The attacks are referred to as energy or sleepless torture [2]. It's the attack. In addition, implementing protective solutions for MANETs is a difficult restriction.

Capacity constraints for memory and processing: Handheld ad hoc nodes have restricted storage resources and machine capacity. It is also difficult to incorporate increasingly complex security technologies like symmetrical or asymmetrical encryption.

Physical disadvantage of mobile devices: mobile devices used in MANETs are light and lightweight, usually in mobile network applications. Computers and data stored on equipment can be easily hacked, which is a loss. For both devices and details, safety measures should be used.

SECURITY ISSUES

We divide risk and safety into two groups in ad hoc networks, including attacks and misconduct.

Attacks

All network damage nodes will be attacked. They can be differentiated by their roots or existence. An actively based division divides crimes into passive and aggressive acts in two groups, both externally and interdependently.

External attacks: Node attacks that cannot reach the logical network. Internal attacks are malicious or disabled attacks performed by an internal node. It is a problem because it is difficult to defend against compromise and malicious internal nodes. It is more troublesome.

Passive attacks: Passive attacks are a permanent collection of data that is later used to launch active attack. The intruders track and inspect packages to collect the necessary details. Because of its widespread presence, the attacker is more likely than conventional wiring environments to launch an attack in this area. The security feature to be given here is confidentiality of information.

Active Attack: nearly all other attacks caused by active contact with people include sleep without battery torment. One of them is responsible for contact between two people and maskers, as one of them. For example, most attacks have led to denial of service (DoS) that degrades or fully prevents communications between nodes. This is a problem caused by active interaction with victims.

Weak intervention

Misbehavioral threats are described as an inappropriate behavior of an internal node that can inadvertently harm another, i.e. that the node does not start an attack, but has other aims like unfair advantages over other node ones. For example, the MAC protocol cannot be executed correctly for higher bandwidth or packages can be executed by other people to store resource and force them to pass on to their own parcels. You may not be able to fully execute them. Until now, basic safety standards have been introduced in MANETs. We will review the current protection areas for MANETs in the following sections and explore new issues and solutions.

ISSUES AND SECURITY CONCERNS IN ROUTING

Roads between nodes to pass data packets to the final destination are found for MANET routing protocol. In comparison to conventional network routing protocols, MANET Routing protocols must be adjustable for functions previously shown in particular for regular network topology changes. The MANÉT Task Force [3] in particular discussed the difficult issues associated with ad hoc network routing. These trials resulted in multiple protocols [4], respectively, that can be categorized as proactive (tabulated) and reactive (on request). The survey [5] reactive protocols reveals that they are more MANET adaptable than pro-active protocols. All these solutions have the problem, however, of trusting all nodes and not being responsible for security. Protecting the routing protocol is very critical. If you can subvert your routing protocol and change your messages in transit the protection of data packets at the highest level cannot be breached. The recently suggested routing of MANET [6] involves many protocols that are secure. In [7] some of these options were discussed. This section deals with the safety problems of routing protocols. We present a list of attacks on conventional MANET routing protocols, in line with two of the DSR and AODV protocols involved, and discuss the new solutions suggested.

DSR AND AODV

A general overview of the protocols for the DSR and AODVs of the working group for the IETF MANET [3] are given in the following sections. Both protocols are important to clarify since they address attacks in general.

DSR

The DSR [4] protocol is based on the approach of the source path. This approach is primarily focused on the selection of the entire route by the source and on each packet sent. The source paths learned are found in each node cache. Initially, when sending a packet, it looks for such a path in the cache. If no cache entry is found, a road discovery network (RREQ) for transmitting to the appropriate location will be started. The RREQ Cache Node is sent to the RREQ destinations by a (RREQ) route, which leads to the RREQ packet route response (RREP). However, the node is added and broadcast its RREQ address continuously, if the correct path is missing. If a node detects a defect in the road, the connection is based on the Routes Detection Mechanism (RER).

AODV

The AODV [7] is a protocol for hop-by routing. If a node is required to send a data packet to a target that does not have a route, then an RREQ is sent to its neighbors, and each neighbor does so until it reaches a valid node's destination or route. This node sends an RREP packet going to the source in the opposite direction. When this response is obtained, every middle man updates his or her routing table. This is the way to construct a path from the source to the destination. Compared to the DSR, an outbound package is not imposed on the whole route; the next hop after each hop is determined separately. AODV assigns routing numbers monotonously to the determination of routing freshness and hops that define the optimal route by their reliability to the theories of vector distances [7].

POSSIBLE ATTACKS AND THREATS IN ROUTING PROTOCOL

There are several different types of attacks in MANETs, which were previously proposed for routing. Wired networks still operate [8]; however, there can be strengthening of existing, strong infrastructures. In this section several attack groups for ad hoc protocols were identified and evaluated. These attacks are covered by AODV and DSR protocols that are used in ad hoc on request protocols without loss of generality. Nearly all conventional protocols on demand are nevertheless susceptible. We presume that MANET is not subject to the table-driven method, so that it is excluded.
Downgrade attacks to Modification Traffic Network can be diverted by manipulating routing data [9], e.g. by modifying data control fields for data packets or submitting false message values to routing attacks. Many attacks on modification were now comprehensive. Routing sequences have been modified: such protocol routing, such as the AODV [7], instantiates, maintains and assigns route sequence numbers that are monotonously expanding. Any node may therefore redirect traffic by claiming a route with a sequence number greater than the actual value.

Figure1: An Ad hoc Network

Take the example of Fig. 1 [10]. Suppose a malignant M node gets the RREQ from S to Target X from B after a route discovery. A RREP with X sequence numbers far higher than the last value of the X will be removed by delete the traffic in the B direction. Finally, a node with a valid route to X through B and a valid RREP is transmitted to S. But B already obtained the mistaken MREP at that point. If the sequence number in the false RREP is higher than that in the true RREP for X, B drops the correct RREP to block the valid path. Consequently, all traffic for X passing B is directed towards M. The higher sequence number for a correct RREQ or RREP for X is the only way to overcome this condition. Hop Account Adjustment: many ad hoc routing protocols, for example, use a hop-count field. Therefore, malicious nodes increase the risk that the hop counter-field of the RREQ will be re-established in a new path. Such an attack, combined with spoofing, is most dangerous. The redirection attack can be performed even if numerous protocol metrics are used. In that case, the attacker must set the field to measure the metric instead of the hop count.

Spoofing Attacks

Spoofing occurs in the event that the resulting parquets change their MAC or IP Address, when a node misrepresents your network identity. This attack can be easily combined with adjustments. Both of these attacks would lead to substantial misinformation, such as, if combined, the establishment of loops[11].

Attacks by Fabrication

This class includes attacks for error message generation. It is difficult to identify these attacks. Road error fabrication: on-demand route maintenance protocols for recovering breakage node mobility paths such as AODV and DSR. The upstream node (predecessor) of the link sends S back a radar packet when the active route from S to D node is broken down. If the latter does not have another route for the D and no path to this place is required, there will be a new route discovery. This weakness could be triggered by the delivery of fake pathway and additional overheads which could lead to sleep deprivation. Routing attacks would break the legal roads. Flash routes: the routing cache table of the node in DSR can be modified with information sent by the node in packet headers. Incredible package paths can also be taught. The risk is that an intruder will easily circumvent this method of learning and poison the neighbor's road caches through the transfer of false routes. Hu et al have recently described a new attack called a rushing attack. Attack Rush: only one RREQ, the first usually in order to restrict overall node discovery in virtually every routing protocol, has been generated on demand. You can easily use this property by sending RREQs. If the RREQs passed to the target'sneighbor, the attacker will provide a route from this path discovery. If a target neighbor receives the hurried RREQ, an RREQ will be sent by the intrusion system and the road survey will no longer send RREQ. In exchange, the initiator does not find routes using at least two hops (three nodes, i.e. route not involving the attacker). Generally speaking, an RREQ attacker can start this attack and pursue all routes discovered faster than legitimate nodes. Each RREQ can be used for any route discovery protocol to hurry up an attack. The attacker does the same even if the sections he sends are balanced by his function [12]. But we agree that in the next debate, the first RREQ obtained will be expressed in nodes. How do RREQ packet rush attackers initiate a rush attack? One or more malicious nodes can use:

1. To prevent interference with protocols for MAC layers or network layers, delete MAC or network delay in packet exchange with the packet transmission delays. An assailant may then refuse these delays in forwarding the appeal.

2. Transmit higher power RREQs: RREQs spanning broader power ranges than other Nodes can be transmitted by powerful physical contact supporters. Generally, the technique does not permit the perpetrator in comparison to other techniques to incorporate him in one discovered direction, so he can't get the RREP (except where the recipient is extremely sensitive). It does not, however, detect legal paths.

3. Two attackers may use a high-quality tunnel [13] to reach their final destination before other RRE Qs. This can be accomplished by wormhole technology [14] when one node is nearer to source and the other is nearer to the target and when two nodes (e.g. wired network) are highly quality track. A high-quality, special route for this attack, which is different from a tunneling attack, is required before wireless multi-hop routes are used.

SUGGESTIONS AND SOLUTIONS

Authentication

Authentication techniques are implemented at all routing levels in order to avoid the involvement of attackers and unauthorized nodes. Many of the solutions proposed in this class change existing authentication routing protocols [14]. The solutions are based on a CA which consists of a trustworthy certificate server with a Public Key known a priori to all nodes, due to digital signatures. This dependency on a fixed server limits the centralization and versatility of the solution. This strategy mostly takes advantage of the exclusion from routing of externally unauthorized nodes so that previous attacks when an external node is started are avoided.

The metric confidence level

Djenouri et al. [15] Describes a new trust value method that regulates the actions of the protocol. This measure must be enforced in control packages to represent the minimum sender trust value. A node that receives a packet may therefore not process or transmit without the required faith in the packet. The authors developed an AODV protocol, SAR, based on Hierarchical Trust Aware Routing.Authentication and metric definitions: This measure is also used in the SAR to choose routes where the necessary trust value is reached by a number of routes. The authors use the military context to clarify the trust values of nodes in a certain confidence level. However, since the network has no hierarchy, the confidence values of the nodes can hardly be calculated. The authentication technique needs to be hierarchically shared. The advantage of this approach is that internal node attacks at a higher degree of trust are not carried out compared with the previous approach.

Verification of Stable Neighbor

Before claiming a neighborly status, the approach requires a three-ways authentication of the communication between two nodes. The well-funded node ignores the other node and does not process the packets it sends if the exchange does not work. This means that high power ranges are used illegally to launch hasty attacks. The next stage of the screening cannot be achieved and is ignored [15] because the broadcaster cannot get the packet from other nodes. The only downside is that it enhances versatility.

Transmission of random messages

Djenouri et al. [15] are proposing this strategy to reduce the possibility of a rushing opponent controlling a return course. The receiving node moved the first RREQ to the regular RREQ and immediately discarded these RREQs. This method uses a node to collect several RREQs and select a random RREQ. This technology therefore comprises two parameters: firstly, the number of RREQ packets to be obtained and then a timeout algorithm. We suppose that the drawback of this strategy is to delay road detection since each node must be waited for a timeout or a number of packets before RREQ are sent. Random selection also prevents appropriate routes from being found. The optimal path can be described, but not modified as hop, power efficiency or other metrics. The direction is optimized.

CONCLUSION

In this paper, many security concerns in MANET is showed that the basic characteristics of a new environment of new network nodes are more dangerous, the solutions for traditional networks are either not directly applicable. There have also been a variety of concerns about various aspects. Intrusion detection systems (IDSs) were implemented that are necessary if preventative measures have failed. The complexity of the problem is increased by the MANET features, which created a wide field of study. The host is focused on the full or partially abnormal appearance of MANET IDS. The fair sharing of traffic monitors and IDS tasks with low-threat networks might not be appropriate. Methods focused on clusters indicate that cluster heads are divided into clusters. Overhead is however, particularly important if the node increases mobility. Additional research is required on the efficacy of this method. MANETs are also of great significance because they are unable to distinguish the ordinary from the exception. Therefore any initiation requires a realistic learning phase. This network is unable to handle complex ad hoc networks.

Finally, with a special form of ad hoc network, safety issues were addressed in WSN. This highly restricted environment poses the difficulty of adapting to ad hoc networks the new protocols. Our opinion is that the latest mechanism, including their new model for communication that takes WSN's special features into account, would be a more judgmental approach.

REFERENCES

[1] W. Stallings, Cryptography and Network Security Principles and Practices, 3rd ed., Pearson Education Inc., 2003.

[2] F. Stajano and R. Anderson, "The Resurrecting Duckling: security issues for ubiquitous computing," in Computer, vol. 35, no. 4, pp. supl22-supl26, April 2002, doi: 10.1109/MC.2002.1012427.

[3] The IETF Web site, http://www.ietf.org
[4] S. Alaparthi, S. R. Parvataneni, C. S. Vaishnavi, P. Sathvika, M. Chandrika and P. Sharanya, "Dynamic Source Routing Protocol—A Comparative Analysis with AODV and DYMO in ZigBeebased Wireless Personal Area Network," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 1042-1046, doi: 10.1109/SPIN.2019.8711689.
[5] R. Meena and L. Tharani, "A re vie w stud y of lightweight proactive source routing protocol for MANETs," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1030-1034, doi: 10.1109/ICGCIoT.2015.7380615.
[6] M. Asch, P. F. Seymour, J. Ernst and D. Gillis, "Incorporation of Node Mobility in Data Replication Schemes in Mobile Ad Hoc Networks," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 0230-0236, doi: 10.1109/IEMCON.2019.8936268.
[7] Y. Shibasaki, K. Sato and K. Iwamura, "An AODV-Based Communication-Efficient Secure Routing Protocol for Large Scale Ad-Hoc Networks," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2020, pp. 1-6, doi: 10.1109/CCNC46108.2020.9045743.
[8] K. Dhanya, C. Jeyalakshmi and A. Balakumar, "A Secure Autonomic Mobile Ad-hoc Network based Trusted Routing Proposal," 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, Tamil Nadu, India, 2019, pp. 1-6, doi: 10.1109/ICCCI.2019.8822012.
[9] C. Pathak, A. Shrivastava and A. Jain, "Ad-hoc on demand distance vector routing protocol using Dijkastra's algorithm (AODV-D) for high throughput in VANET (Vehicular Ad-hoc Network)," 2016 11th International Conference on Industrial and Information Systems (ICIIS), Roorkee, 2016, pp. 355-359, doi: 10.1109/ICIINFS.2016.8262965.
[10] M. M. E. A. Mahmoud, X. Lin and X. Shen, "Secure and reliable routing protocols for heterogeneous multihop wireless networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 1140-1153, April 2015, doi: 10.1109/TPDS.2013.138.
[11] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," 10th IEEE Int'l. Conf. Network Protocols (ICNP '02), Nov. 2002.
[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Wksp. Wireless Security WiSe 2003, San Diego, CA, USA, Sept.2003.
[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," 22nd Annual Joint Conf. IEEE Comp. and Commun. Societies (INFOCOM 2003), Apr. 2003.
[14] S. Yi, R Naldurg, and R. Kravets, "Security-aware Ad-hoc Routing for Wireless Networks," ACM Wksp. Mobile Ad Hoc Networks ,Mobihoc, 2001.
[15] D. Djenouri and N. Badache, "New Power-aware Routing for Mobile Ad Hoc Networks," accepted in the Int'l. J. Ad Hoc and Ubiquitous Computing (Inderscience), vol 1, no. 3, 2005.