University of Ngaoundere
Faculty of sciences
Department of Mathematics and computer sciences

Université de Ngaoundéré
Faculté de sciences
Département de Mathématique et informatique

TPE
SECURITY SYSTEM AND NETWORK

Theme N° 02 : **SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS - A SURVEY.**

R. Nandakumar and k. Nirmala
Australian journal of basic and applied science, issn:1991-8178 eissn: 2309-8414

Summarized by

Names	Level	Students matricule N°
AWÉ SAMALNA DENIS	M1SLED	07L251FS
SAMDALLE AMARIA	M1SLED	09B051FS

Under the coordination to :
Dr.-Ing. Franklin TCHAKOUNTE
University of Ngaoundere

Academic Year : 2016-2017

1. Introduction

a. Context

For our ongoing century, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handset digital devices, has impelled a revolutionary change in the computing world: computing will not merely relay on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [Marco C., 2003]. A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [M.S. Corson, 1999]. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension.

b. Background

- **Description**

There are some ultimate goals regarding security solutions with respect to Mobile ad hoc networks or we can say there are some security services which should be fulfill in order to enforce security like authentication, confidentiality, integrity to mobile users.

The wireless medium as compared to wired network node mobility more dynamics in mobile ad hoc networks [Muh. & Yas., 2011]. The network topology is highly dynamic due to free movement in the network like nodes can frequently join or leave, as well as in the network by their own will. There are also interferences in the wireless channel due to this way error, exhibiting volatile characteristics in terms of bandwidth and delay occurs. Due to such dynamic behaviors mobile users request for security services at any anytime or anywhere whenever they move from one place to another in the network.

- **Challenges**

There are some characteristics of security solutions of MANETs which will clearly provide security solutions with respect to network protection and also provide desirable network performance [Muh. & Yas., 2011]. Some of these challenges can be resumed below:

1. The security solution should also implement across many individual components in order to provide collective protection to secure entire network. In terms of computation capabilities are concerned like energy supply, memory as well as communication capacity each device has to work within its own.

2. The security solution should also provide security with respect to different layers of the protocol stack and each layer provides line of defense. It is also not possible that only one single-layer solution can handle all potential attacks.

3. The security solutions should avoid threats from both outsiders as well as inside. According to outside attacks are concerned it should avoid attacks on the wireless channel as well as network topology where as in case of inside attacks are concerned an intruder who enter into the network through compromised devices and gain access to different network knowledge.

4. The security solutions should enforce all three components of security like prevention, detection, and reaction.

5. The security solutions should be affordable as well as practical in resource constrained and highly dynamic networking scenario.

- Routing protocol description

There are basically three kind of routing protocols which are:

Table driven routing protocols

In these routing protocols each node in the network maintains the complete routing information of the network by occasionally updating the routing table, so when a node needs to send some data or information, so there is no any kind of delay for discovering the route in the whole network [Muh. & Yas., 2011]. This type of routing protocols approximately works the same way as the wired network routing protocol works. The table driven protocols are DSDV and WRP.

On-Demand routing protocols

While in this kind of routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets [Muh. & Yas., 2011]. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used.

Hybrid routing protocols (ZRP)

In this type of routing protocol is the combination of the above two categories. In which nodes belonging to a particular geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol [Muh. & Yas., 2011].

All said, these background studies helped us to understand the possible challenges that exist in the implementation of MANETs. Especially due to the constant changing nature of the topology and possible attacks resulting from communication between nodes in this type network.

As a summarized functional stack, we noticed the figure below:

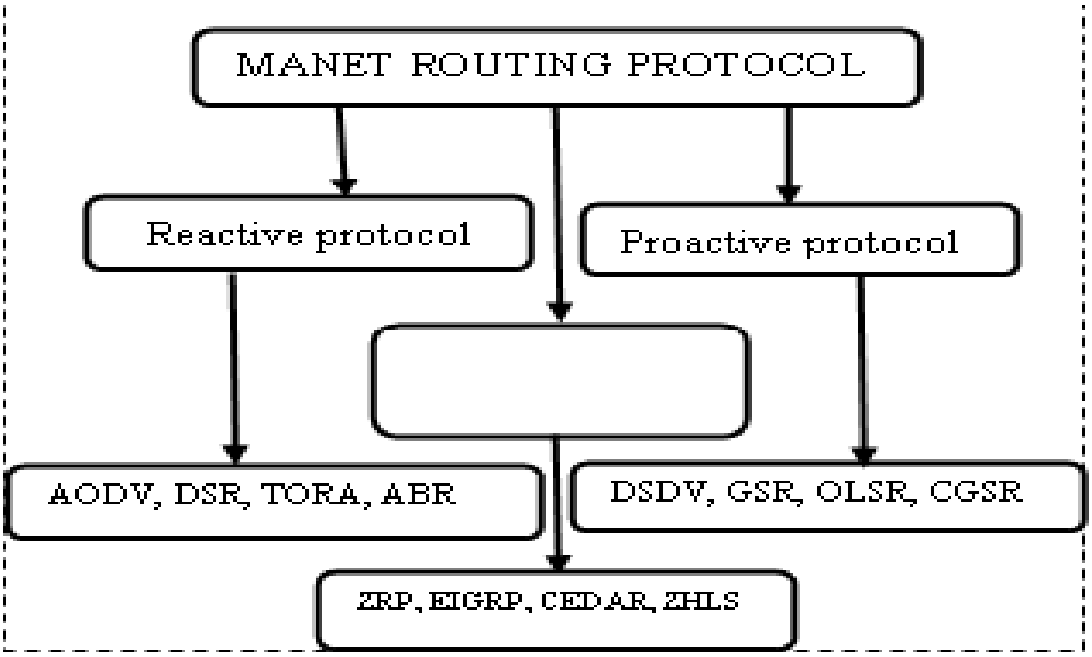

Fig. **MANETs routing protocols** [Indrajeet K. & al, 2014]

These led us to deduce the following problems and derive research questions.

Problem and research questions

The fact that Ad hoc network can be created on the spot, each node in the Ad hoc network has both routing and hosting abilities. The security challenges arise due to MANET's self-configuration and self-maintenance capabilities [M.S. Corson M., & al., 1999] As opposed to the wired networks, wireless networks are characterized by a number of complex challenges related to security boundaries, which can be justified due to: open peer-to-peer, network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology [Zaiba I., 2011]. The main research question is how to develop solutions to the attacks to which MANETs are exposed.

2. RELATED WORKS

Mobile Ad hoc Networks is a new evolutionary and innovative branch in networking. Due to that, many research works have been carried out, exploring almost all the aspects of this mobile network. With regard to security challenges in Mobile Ad hoc Networks, we went throw some of the related works, as presented in form of a comparative table with as evaluation criteria : the security features studied, the level of extendibility, advantages and disadvantages. This table is not exhaustive, since we limited ourselves only on ten recent works.

WORKS	PROPOSED SCHEMES	SECURITY FEATURES	SCALABILITY	ADVANTAGES	DISADVANTAGES
Zaiba Ishrat IJCS, 2011	Security issues, challenges & solution in MANET	typical and dangerous vulnerability in the MANET, attack types security criteria	low	Proposes solutions to black hole, worm hole and impersonation and repudiation attack	Still some security challenges on the protocol stacks
E. Gajendran , S.Vijayan and B.Sarvesan, IJCA, 2013	A Literature Survey on Security Challenges in Mobile Ad Hoc Networks	Security Attacks on each layer in MANET and problems existing in secured routing algorithms	moderate	Good exploration of routing algorithms both for stable and constant varying networks	No defined set of formalize criteria to evaluate identification process.
Indrajeet Kumar1, Varun Prabhakar2, Jyoti Rawat3, Noor Mohd IJERST, April-2014, pp: (108-114)	A Conventional and proposed model for comparative study of security breach attack in Mobile Ad hoc Network	types of possible attack and comparison between available security protocols	high	Good comparison of Various Secure Routing Protocols.	Most of the routing protocols are on demand.
Ali D., Reza K. and Esmail k; IJCSES, Vol.6, No.1, February 2015	SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY	Defeating approaches MANETs attacks	high	Solutions for sniffing, dynamic frequency, redundancy and encryption	Evaluation of processing time and absence of centralized control key distribution

G. Jose Moses, Prof.P.Suresh Varma, N.Supriya, G.NagaSatish; ijcnis. avril 2012	Security Aspects and Challenges in Mobile Ad hoc Networks	Construction of security mechanism from a study of passive and active attacks	moderate	Good description of security challenges related to active attacks.	No formalized solution to passive attacks
Dr.Satya Prakash Singh & Ramveer Singh	Security Challenges in Mobile Ad hoc Network	Exploring of security features	High	Important control of traffic in MANETs	Solution to attacks on routing protocols
S.banu priya, c.theebendra., IJRCAR issn 2320-7345	A study on security challenges in mobile ad hoc networks	Analysis of security attacks	High		reducing packet over head and processing time
Amer O. & Hebatallah A.	Mobile Ad-hoc Network Simulators, A Survey and comparison	Security challenges related to Communication medium in MANETs	High	-extend security solution of wired networks to the MANETs.	-no measures for newly belt medium of networking.
Ashish kumar khare1, Dr. R. C. Jain2 and Dr. J. L. Rana3	A REVIEW: TRUST, ATTACKS AND SECURITY CHALLENGES IN MANET	maintain a stable, secured, trustworthy group of movable nodes	high	Solves intrusion threats and attacks related to scalability	maintaining the record to provide appropriate certification for the arriving node(s)

Table1. Comparative table on related works

3. METHODOLOGY EMPLOYED

To come about this survey, the author decided to describe the constituency of Mobile Ad hoc Networks. Some of the characteristic elements studied are: Autonomous behavior (In MANET, each node acts as both host and router), Multi-hop transmission (When a source node and destination node for a message is out of the transmission range, the MANETs are capable of multi-hop transmission), Distributed nature of operation (As a centralized control is absent here, the control and operation of the network is distributed among the nodes), Dynamically changing topology (Due to mobile nodes, the change in topology is frequent and dynamic in nature), Inferior link capacity (The reliability, scalability, efficiency and capacity of wireless links are often inferior when compared with wired links.), Symmetric environment (All nodes have identical features with similar responsibilities and capabilities.), Light weight features: (MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage) and Absence of Infrastructure (Ad-hoc networks are supposed to operate independently of any fixed infrastructure).

Later introducing the different domain of application of this new technology in everyday's life such as in maintaining an information network among the vehicles, soldiers and military head quarters, emergency/rescue operations for natural calamities relief efforts, e.g. in fire, flood, or earthquake, linking an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference and the intercommunication between various mobile devices (such as a mobile phone, laptops, and wearable computers)

In the process of describing the different routing protocols of MANETs, we will discover the various challenges just to cite some examples we have Routing, Security and Reliability, Quality of Service, Inter-networking, Power Consumption, Multicast, etc. Challenges among which the particular case study of security challenge led to the proposition of two solutions, namely packet leashes and non-repudiation security criteria that deals respectively with wormhole and blackmail attacks.

4. RESULTS FOUND AND PERSPECTIVES

This technology due to numerous geographical instabilities and nowadays war crews, is becoming an interesting research topic and is an open door to research projects. This Mobile Ad hoc Networks bring a great opportunity together with many challenges.

This paper brought about great discoveries on the different challenges related to the security of this constantly changing form of networks (that is MANETs). Appreciable outcomes of this survey help us to realize that some of the attacks can be prevented, thanks to some applied concepts. Such as:

- The non-repudiation Security criteria, which can help to solve the problem of Blackmail on MANETs;

- The packet leashes, which prevents eventual Wormhole attacks on MANETs;

Nevertheless many open research issues, according to the author, are available, in order to resolve most of the serious cases such as

- Attack on the security of MANETs that are still uncontrolled. For example: the problem of attacks using fabrication generates false routing messages. Such types of attacks are the described to be very difficult to detect. Therefore reducing packet overhead and processing time, besides increasing accuracy is an important challenge. By increasing accuracy, it can detect cooperative malicious nodes.

- Redundancy approach, generate lots of duplicated packets and waste nodes resources. Also it increases congestion and packet lost [M.S. Corson, 1999]. Effectively choosing number of duplicated paths, based on risk level, is highly challengeable. Also combining this approach with some other approaches in order to detect malicious nodes is another challengeable issue. Dynamic frequency is effective in multi-type MANETs. By using this approach in multi-type MANET, each node secures its packets by sending in different frequencies. In addition, breaking one frequency has no effect on others. This is a challenge in this approach.

5. MOST IMPORTANT PUBLICATIONS FOR THIS WORK

- **[Ali D. & al., 2015]** Ali D., Seyed R. and Esmail k., Security Challenges In Mobile Ad Hoc Networks: A Survey**,** (IJCSES) Vol.6, No.1, February 2015
- **[Indrajeet K. & al, 2014]** Indrajeet Kumar1, Varun Prabhakar2, Jyoti Rawat3, Noor Mohd., A Conventional and proposed model for comparative study of security breach attack in Mobile Adhoc Network, International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463 Vol. 3 Issue 4, April-2014, pp: (108-114).
- **[Jose G., & al., 2012]** G.Jose Moses, P.Suresh Varma, N.Supriya, G.NagaSatish, Security Aspects and Challenges in Mobile Adhoc Networks, I.J. Computer Network and Information Security, 2012, 6, 26-32
- **[M.S. Corson M., & al., 1999]** M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.
- **[Marco C., 2003]** Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
- **[Muh. & Yas., 2011]** Muhammad Arshad Ali & Yasir Sarwar Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions, March 2011.
- **[Shabbir & al., 2015]** Shabbir, A., Khalid, F., Shaheed, S.M., Abbas, J. and Zia-Ul-Haq, M. (2015) Security: A Core Issue in Mobile Ad hoc Networks. Journal of Computer and Communications, **3**, 41-66. http://dx.doi.org/10.4236/jcc.2015.312005
- **[Zaiba I., 2011]** Zaiba Ishrat, Security issues, challenges & solution in MANET. IJCST Vol. 2, Issue 4, Oct 2011.