International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876, Impact Factor: RJIF 5.44
www.engineeringresearchjournal.com
Volume 2; Issue 2; March 2016; Page No. 55-58

A survey on security challenges handled in Manet cloud computing

SM Thokale

Prof Computer Dept PREC, Loni

Abstract
Security has become a primary concept in order to provide protected communication between mobile nodes in a hostile environment. Recently there has been much research activity in the emerging area of intermittently connected ad hoc networks and delay tolerant networks. There are different types of delay tolerant n/ws, depending on the nature of the network environment. Routing in delay tolerant n/ws is one of the key components in the Delay Tolerant N/w architecture. Trust is an important aspect of mobile ad hoc n/w. It enables entities to cope with uncertainties and uncontrollability caused by the free will of others. Trust computation and management are highly challenges issues in Mobile Ad hoc N/ws. This report also discusses different no of scenarios of Mobile Ad hoc n/w which we implement in our simulation. The role of infrastructure-less mobile ad hoc n/ws in ubiquitous n/ws is outlined. In a Mobile Ad hoc N/w there are no dedicated routers and all network node must contribute to routing. Classification of routing protocols for Mobile Ad hoc N/w is based on how routing information is acquired and maintained by mobile nodes and on roles of n/w nodes in a routing. Now a days Mobile Ad hoc N/w are most technique in computing mobile. This paper focused on the evolution of the Mobile Ad hoc n/w, the challenge in it and a wide area of itâ€™s applications. the first section provide a brief info about the history and evolution of Mobile Ad hoc N/w, next to it discuss the major challenges in Mobile Ad hoc N/w and towards the end mentioned some of the application of Mobile Ad hoc N/w.

Keywords: MANET, routing protocols, security, challenges**.**

1. Introduction

Wireless networks have become increasingly popular in the past ten years, particularly within the 1990's when they are being adapted to enable mobility and wireless devices become popular. As the popularity of mobile devices and wireless networks significantly increased over the past years,

Wireless ad hoc n/w has now become one of the most vibrant and active fields of communication and networking research. Gives us many intriguing future applications of mobile ad hoc n/ws, there are some critical challenges to be solved. Thus, this paper present an overview of the history of Mobile Ad hoc N/w. It represent several challenging issues and the

Future work. The use of mobile services is an evolution from the technical and marketing points of view. From the technological point of view, convergence can be achieved at three levels: the terminal level, the intelligent network (IN) level. However, Experts and new member find that they cannot easily integrate all the current switches. The level in which significant progress has been achieved is the IN level. Solutions based on the IN exactly fit market demands for flexible, innovative services and fast introduction to the market. Hence, adoption of an IN solution by mobile operators and implementation of wireless access solutions by fixed network operators are the current key drivers towards fixed-mobile convergence (FMC).

N/w layer routing and data forwarding protocols (e.g., ad hoc routing). Accordingly, we focus on the link and n/w layer now a days mobile ad hoc n/ws have received tremendous attention because of their self-configuration and maintenance capabilities. While early research assumed a friendly and cooperative environment and focused on problems of wireless channel access and multi-hop routing, security is a primary concern in order to provide protected communication between nodes in a potentially environment. Although security has long been an active research topic in wire-line networks, the characteristics of mobile ad hoc n/w present a new set of nontrivial challenges to security design. Challenges include open n/w architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Similarly, the existing security solutions for wired networks do not directly apply to the mobile ad hoc n/w domain. The main goal of the security for mobile ad hoc n/w is to provide security services, such as authority, privacy, duplication, and presence to mobile users. In order to achieve this goal, the security solution must be provide complete authorization spanning the entire protocol stack. Table describes security issues in each layer. This article describes a fundamental security problem in mobile ad hoc n/w the authorization basic aim to deliver data bits from source to destination. In other words, to protect the network connectivity between mobile nodes over multi hop wireless channels, which is the basis to support n/w security services. Multi hop connectivity is provided in mobile ad hoc n/w through following steps: [1]. ensure one hop connectivity through link layer protocols (e.g., wireless MAC) and [2] extends connectivity to multiple hops through security issues, challenges, and solutions in mobile ad hoc n/w in this article.to periodically evaluate the trust value of node based on some metric and computational methods. Trust computation in n/w are relatively simpler because the trust value here changes mainly due to behavior of nodes. After observations these behaviour are predictable. Mobile ad hoc n/w got outstanding success as well as tremendous attention due to its maintenance and configuration properties or behavior. At early stage mostly people focused on its friendly and cooperative environment and due to this way many different problems came in being; security is one of the

primary concept in order to provide secure communication between different nodes in a mobile ad hoc n/w environment. Due to different characteristics of Mobile ad hoc n/w security is an active research topic in wireless path, which is also a nontrivial challenging to security design. There are different types of challenges in mobile ad hoc n/w which are given below:

1. Open network architecture
2. Shared wireless medium
3. Stringent resource constraints
4. Highly dynamic network topology

It is also true that the solutions to the wired networks do not workable to mobile ad hoc networks domain. It is also true that security has long been an active research topic in wireline networks; but due to unique characteristics of mobile Ad hoc N/ws there are many challenges because of its self-organizing behavior. These challenges are shared wireless medium, highly dynamic network topology, stringent resource constraints and open network architecture. Itâ €™s true that existing security solutions for wired networks do not directly apply to the Mobile ad hoc networks domain. Mobile ad hoc network has different challenges with respect to wireless security due to some of the following reasons:

1. The wireless network especially liable to attacks because of active eavesdropping to passive interfering.
2. Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
3. Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
4. Due to mobile Ad hoc N/ws â€™s properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider attacks in mobile Ad hoc N/ws, in which insider attacks are more difficult to deal with.
5. It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

Routing Protocols for Mobile Ad hoc N/ws Research on mobile Ad hoc N/ws has nearly 20 years focused on routing and this focus still remains. Several routing protocols for mobile Ad hoc N/ws have been proposed and some surveys on these protocols have been published and an IETF Routing Area Working Group mobile Ad hoc N/ws has been active for a decade with six currently active Internet drafts. Routing protocols for mobile Ad hoc N/ws are usually classified into table driven/proactive protocols, on- demand/reactive protocols, and hybrid protocols based on how routing information is acquired and maintained by mobile nodes. Table driven/proactive protocols use a proactive routing 370Karlsson, Dooley, & Pulkkis scheme, in which every network node maintains consistent up-to-date routing information from each node to all other nodes in the network. On-demand/reactive protocols are based on a reactive routing scheme, in which at least one route is established only when needed. A hybrid routing protocol is a combination of proactive and reactive schemes with the aim of exploiting the advantages of both types of protocols another classification into uniform and non-uniform routing protocols for mobile Ad hoc N/ws is based on the network node roles in a routing scheme. In a uniform routing protocol all network nodes have the same role, importance and functionality. In a non-uniform routing protocol some network nodes carry out distinct management and/or routing functions. A uniform routing protocols is either reactive or proactive, while different classification schemes have been proposed for non-uniform routing protocol (Feeney, 1999; Liu & Kaiser, 2005)In this section some relevant reactive, proactive, and hybrid routing protocols for mobile Ad hoc N/ws are presented. Table Driven/Proactive Protocols Typical table driven protocols are highly dynamic Destination-Sequenced Distance Vector Routing (DSDV) (Perkins & Bhagwat, 1994) and Optimized Link State Routing (OLSR) (Clausen & Jacquet, 2003).Table driven routing protocols have a low route acquisition delay because every node always has a fresh route to all other nodes in the network. However, the storage, bandwidth, and power requirements are high since each node must keep its routing table up-to date (with route information to all other nodes) which mandates periodic routing message exchanges (Mohseni *et al*. 2010). On Demand/Reactive Protocols On-demand protocols incur a much lower load on the network, compared to table driven, since each node does not need to constantly keep their routing tables up-to-date. However, route acqui- sition delay is high since routing messages must be exchanged every time before communication is possible over a new route (Mohseni *et al*., 2010). Two prominent mobile Ad hoc N/ws routing protocols, based on reactive routing schemes, are Ad hoc On-demand Distance Vector (AODV) (Perkins *et al*., 2003) and Dynamic Source Routing (DSR) (Johnson *et al*., 2007), which will now be respectively considered. Ad hoc On-demand Distance Vector (AODV) In AODV, when a node wants to communicate with another, the source node floods the network with route request (RREQ) messages. If a node that receives a RREQ packet is not the destination or doesn't have a fresh route to the destination it creates a reverse route to the source If the receiver of a RREQ is the destination node, it sends a route reply message back to the source as a unicast packet over the route it received the RREQ. The destination node only sends a RREP to the first RREQ message it receives. Every node receiving a RREP also creates a route to the destination in the routing table. As a result, when the RREP reaches the source, all nodes in the shortest route path will have a route both to the source and destination.

Dynamic Source Routing As with AODV, DSR floods the network with route request messages as a result of route discovery initiation. However, compared with AODV, the destination node returns a route reply for security

2. Related work

As the popularity of mobile devices and wireless networks significantly increased over the past years, wireless ad hoc n/ws has become one of the vibrant and active fields of communication and networking research. Given many intriguing future applications of mobile ad hoc n/w, mobile tolerant n/w, there are some critical challenges and open

problems to be solved. Thus, broadly this paper present an overview of the history of Mobile Tolerant N/w

1. A convergence method for fixed and mobile services via a standard based IN platform may provide a step in the right direction. This paper deals with steps for convergence services and their benefits to network operators and customers. It presents possible paths from the existing GSM to UMTS. The paper also provides a comparative analysis of the wireless technologies involved in this evolution
2. Discuss the challenges to security design, and review the state-of-the-art security plans that protect the Mobile Ad hoc N/w link and network layer operations of delivering packets over the multi hop wireless channel. The security solution should span both layers, and include all three security components of avoidance, detection, and reaction.
3. Current developments in era sure coding and n/w coding applied to Delay Tolerant N/ws are also discussed.
4. Analyze various works on trust dynamics including trust broadcast prediction and aggregation algorithms, the influence of n/w dynamics on trust dynamics and the impact of trust on security services.
5. A comparison of existing secure routing protocols form the main contribution in this paper, while some future research challenges in secure Mobile Ad hoc N/w routing are discussed.
6. Wireless ad hoc networks has now become one of the most active and active fields of communication and networking research. As there are many attractive future applications of mobile ad hoc networks there are challenges and open troubles to be solved.
7. Surroundings exact implications on the necessary approach in implementing security in such dynamically changing networks have not yet fully realized.
8. This chapter provides a complete review of attacks beside a specific type of target, namely the routing protocols used by Mobile Ad hoc N/w. We introduce the security issues precise to Mobile Ad hoc N/ws and present a detailed classification of the attacks against these complex distributed systems. Then we discuss various positive and immediate solutions projected for Mobile Ad hoc N/w. We outline secure routing solutions to avoid some attacks against the routing protocols based on cooperation between nodes. We also give a summary of disturbance detection in Mobile Ad hoc N/w. s and specify the nature of IDSs that include planned for Mobile Ad hoc N/ws in the past decade.

3. System Architecture

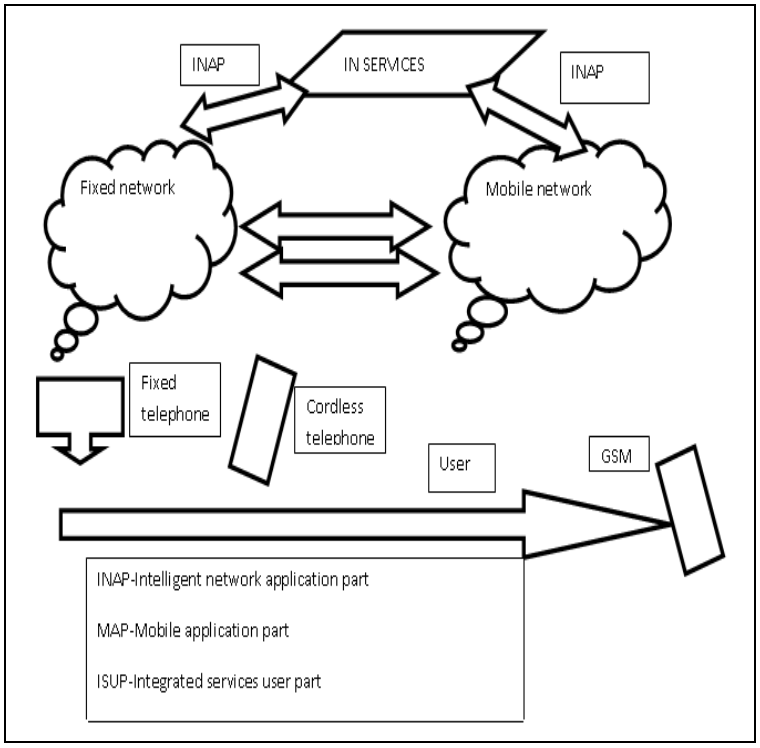

Fig 1: The FMC network infrastructure

Now a days clients are ever more using mobile phones to replace fixed phones, due to cellular phonesâ €™ convenience and greater functionality. The research of the Yankee Group reveals that more than 30 percent of users in some European countries use their mobile phones at home (e.g., 37 percent in the United Kingdom, 38 percent in France). In addition, it is expected that by 2005 mobile service penetration levels of 50â€“90 percent will be achieved in some of the more developed European markets such as Scandinavia, Italy, the United Kingdom, France, and Germany, with an average of 52 percent for the entire European Union (EU) [3]. These trends are stimulating operators and vendors to provide the same services over both set and mobile networks, upward a Converge IN platform (Fig. 1).

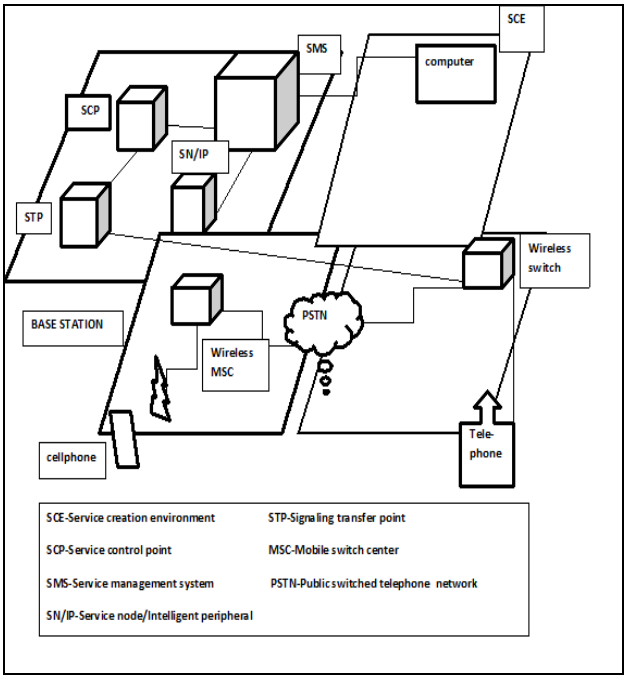

Fig 2: The convergent intelligent network.

Success in providing FMC through a converged IN platform that supports multiple protocols for both fixed and mobile infrastructure ultimately relies on the capabilities of the IN architecture (Fig. 2).

4. Conclusion

Network operators and service providers know that they can succeed only if they develop new markets, enlarge their variety of services. And provide services at a quicker pace and competitive prices. Thus, they have to reduce prepared and service constraints compulsory by different technologies. An emerging solution is a removal of the barrier between various networks by converging fixed and mobile services. Using the fixed-mobile convergence approach, operators and service providers will be able to enhance customer services, and increase their own competitiveness and revenues. This can be done in a cost effective way by upgrading the existing technologies and developing FMC strategies toward third-generation wireless technologies. This article provide an overview of the state of the art on routing protocols in DTNs. Many excellent approaches to addressing the unique problems in DTNs have been reported in the literature. Routing security in infrastructure less and self con figuring mobile networks, such as Mobile Ad hoc N/ws, has been decorated as one of the most challenging security issues in current and future everywhere n/w. Since there are a number of latent Mobile Ad hoc N/w security threats and many network environments. The aim of this paper is to understand the challenges and request of Mobile Ad hoc N/w, so as to improve the research work in this field. During the study we understand that, Mobile Ad hoc N/w are expected to be very useful and important infrastructure for achieve future everywhere humanity Designing Mobile Ad hoc N/w protocols and applications is a very complicated task since it is hardly possible to build largescale and pragmatic test beds in real world for performance estimate

5. References

1. Kavita Taneja1, RB Patel MM. Instt. Of Computer Tech. & Business Management, Mullana, Haryana, India. Dept of Computer Engg. M. M. Engineering College, Mullana, Haryana, India" Mobile Ad hoc Networks: Challenges and Future" Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007) RIMT-IET, Mandi Gobindgarh. 2007, 23.
2. Marija Vrdoljak, Sasa Ivan, Vrdoljak FESB. University of Split Goran Skugor, ERICSSON-Nikola Tesla Fixed-Mobile Convergence Strategy: Technologies and Market Opportunities IEEE Communications Magazine, 2000, 1-16.
3. Haoyang Haiyunluo, Fanye Songwulu, Andlixia Zh. ang, Ucla Computer science department Security In mobile adhoc networks: Challenges And Solutions Ieee Wireless Communications, 2004.
4. Zhensheng zhang, Sandiego research center Routing In intermittently connected Mobile adhoc networks And Delay tolerant networks: Overview and challenges IEEE Communications Surveys & Tutorials, 2006.
5. Kannan Govindan, Member IEEE. And Prasant Mohapatra, Fellow IEEE Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey Ieee Communications Surveys & Tutorials, Second Quarter 2012; 14(2).
6. Muhammad Arshad Ali, Yasir Sarwar. Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions School of Computing Blekinge Institute of Technology 371 79 Karlskrona Sweden
7. Laurence S. Dooley The Open University, Milton Keynes, England Routing Security in Mobile Ad-hoc Networks Issues in Informing Science and Information Technology 2012, 9.
8. Ankur O, Bang Prabhakar L, Ramteke. MANET : History, Challenges And Applications" International Journal of Application or Innovation in Engineering & Management (IJAIEM)
9. Kärpijoki Helsinki. University of Technology Telecommunications Software and Multimedia Laboratory Security in Ad Hoc Networks Seminar on Network Security.
10. Sevil Şen, John A, Clark Juan E. Tapiador Department of Computer Science, University of York, YO10 5DD, UK Security Threats in Mobile Ad Hoc Networks.