A Survey of Manet Governance Survivability on 4g Routing Techniques

Chilakalapudi Meher Babu¹, Dr. Ashish B. Sasankar²

¹Ph.D. Research Scholar, Post-Graduate Teaching Department of Electronics & Computer Science Dept, R.T.M. Nagpur University, Nagpur, India.
²professor., Head, Dept Of MCA, G.H.Raisoni Institute Of I.T, Hariganga Campus, MIDC, Nagpur, India.

Abstract: The various research activities being done by various groups on fourth generation of the cellular system will provide single interface to all kinds of wireless networks allowing participating nodes to access to the network through cellular, wireless LAN networks, and new protocols such as successful and safe implementation of the fourth generation of the wireless technology into the mobile ad-hoc network for the next generation military environment might face tough challenges. It also can be interrupted due to significant differences between the civil and military environment. Physical and technological constraints, geographical limitations and DoS attacks are some of foreseeable challenges. By putting all possible technological advances together from the 4G and MANET, this has set an example for future battle-field. The era of the new wireless communications is very challenging on 4G and MANET communication systems has been emphasized in this paper.

Keywords: 4G, Mobile Ad-hoc Network, Military Wireless Network, m-Governance, 4GWs.

I. Introduction

Due to its vital services, Mobile ad hoc network have become an important part of our life. There are several types of attacks and intrusions targeting wireless networks as directly affect the performance and the survivability of MANETs. Routing is essential service for end-to-end communication in MANET, attacks on routing protocol disrupt the reliability and performance of MANET. It can be divided into two categories,

(1) First is routing disruption attack which the attacker trying to change the course of packets.
(2) Second resource consumption attack

This survey focusing on initiatives which make MANET survives against active attacks including Denial of Service (DoS). The contribution of this survey are:

1) investigation of the most valuable techniques and approaches which support MANET routing survivability;
2) Identification the requirement of routing survivability;
3) Investigation of main DoS which violate availability;
4) The classification of routing survivability in initiatives in three groups: authentication,
5) Path Selection, and attack detection.

DIMENSIONS OF MANET And 4G RESEARCHES

A large body of research has been accumulated to address these specific issues, and constraints. In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain. The research activities will be grouped, according to a layered approaching to three main areas: 1. Enabling technologies; 2. Networking; 3. Middleware and Applications. Also several issues (energy management, security and cooperation, quality of service, network simulation) span all areas.

SECURITY ENHANCEMENT IN MANET WITH 4G

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Authentication research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:
The general concepts of 4G can be present in the list as follows:

- improved capacity,
- increased number of users in the cell,
- lower transmission costs
- connection with already existing systems,
- lower latency,
- based on IPv6 protocol, with packet switching,
- single interface for all wireless connections,
- increased mobility,
- support for media applications,
- seamless connectivity,
- improved security,
- improved and guaranteed Quality-of-Service,
- global roaming of networks,
- standardized open interface,
- self-organizing networks
- fast response

<table>
<thead>
<tr>
<th>Technology/Features</th>
<th>1G</th>
<th>2G/2.5G</th>
<th>3G</th>
<th>4G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Bandwidth</td>
<td>2 kbps</td>
<td>14.4-64kpbs</td>
<td>2 Mbps</td>
<td>2000 Mbps to 1 Gbps for low mobility</td>
</tr>
<tr>
<td>Standards</td>
<td>AMPS</td>
<td>2G: TDMA, CDMA, GSM, EDGE, 1xRTT</td>
<td>WCDMA, CDMA-2000</td>
<td>Single unified standard</td>
</tr>
<tr>
<td>Technology</td>
<td>Analog Cellular technology</td>
<td>Digital cellular technology</td>
<td>Broad bandwidth, CDMA, IP technology</td>
<td>Unified IP and seamless combination of broadband, LAN/WAN/PAN and WLAN</td>
</tr>
<tr>
<td>Service</td>
<td>Mobile Telephony (voice)</td>
<td>2G: Digital voice, Short Messaging</td>
<td>Integrated Higher Quality audio, video and data</td>
<td>Dynamic Information Access, Wearable devices</td>
</tr>
<tr>
<td>Multiplexing</td>
<td>FDMA</td>
<td>TDMA, CDMA</td>
<td>CDMA</td>
<td>CDMA</td>
</tr>
<tr>
<td>Switching</td>
<td>Circuit</td>
<td>2G: Circuit 2.5G: Circuit for access network &amp; air interface; packet for core network and data</td>
<td>Packet except circuit for air interface</td>
<td>All packet</td>
</tr>
<tr>
<td>Core Network</td>
<td>PSTN</td>
<td>PSTN</td>
<td>Packet network</td>
<td>Internet</td>
</tr>
<tr>
<td>Handoff</td>
<td>Horizontal</td>
<td>Horizontal</td>
<td>Horizontal</td>
<td>Horizontal and vertical</td>
</tr>
</tbody>
</table>

II. Manet And 4g With Governance

Governments, at various levels, have noticed the spread of the Internet and Web and interest in using the latest technologies to improve the services strategies and their implementation involving the utilization of all kinds of wireless and mobile technologies, services, applications, and devices for improving benefits to citizens, business, and all government units. Transparency and accountability are the key mantras of a successful government. With growing number of mobile subscriber base, mobile adhoc-Governance has become a powerful tool in the delivery of public services. It's a well known that information and communication technology (ICT) is very critical for processing, storing, organizing, and presenting data and information. The new growth driver now is the mobile phone. It has emerged as an effective tool for good governance in not only facilitating openness and transparency, but also in creating a flow of information between departments, institutions, and various layers of the government. Mobile adhoc-Governance will surely steer the government to a 'service oriented' mindset and make it more agile, responsive, accountable, and action-oriented (Singh, A., 2010).Current mobile adhoc-Governance applications do not exploit the full potential of available technology. In current stage mobile adhoc -Governance is concentrating on following service domains: mobile adhoc–Administration, mobile adhoc-Democracy, mobile adhoc–Education, mobile adhoc – Health, mobile adhoc–Transport, m-Payment. Thus, mobile devices are presently used by governments and public only for the purpose of information sharing. Different mobile adhoc governance Services are identified for pilot level implementation to deliver services through mobile phones and make it accessible to the citizens in the field, in the street, at home or other convenient locations on a 24 X 7 basis, rather than the users having to visit government offices or log on to the internet portals to access services. But, the services such as m-disaster relief/rescue operations (Flood, tsunami, earthquake) Mobile -Education (Virtual classrooms, Conferences) Mobile -Monitoring system (Police raids) Mobile -Excavations Mobile -Intelligent transport system

These service domains can be included in like: Military maneuvers, Mobile robotics, Disaster relief, Home networking, Conferences, and for any instant infrastructure.
MANET CAN BE EFFICIENTLY USED IN SITUATION LIKE SURGICAL STRIKE 26/11, at TAJ HOTEL IN MUMBAI and A SURGICAL STRIKE at UDI AT KASHMIR is a military attack which results in surrounding structures, vehicles, buildings, or the general public infrastructure and utilities provides an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications with survivable, efficient dynamic networking. Rescue workers engaged in disaster relief investigate the extent of the damage around them and collaboratively work by sharing the information on their locations and findings. In a situation like 26/11, commandos inside the TAJ could communicate with the use of MANET and they could be connected with the rest of world by using satellite network. But at that time we were not aware about what was happening inside the building.

MANETS can be used in m-Governance environment in uncertain and unorganized scenarios, the problem of constant connectivity and high transmission quality can be solved by 4G concept. This concept can be explained with help of an example of (26/11) Taj Hotel. In the earlier section, we discussed how MANET can be used in 26/11 Taj Hotel situation. The situation can be further improved if the following improvements can be implemented:

- **Situation 1** - The MANET developed in such a situation can also interact with outer world, So that cops outside the Taj Hotel can get idea of situation inside Hotel an help them in better way.

- **Situation 2** - As nodes can move arbitrarily, there could be a situation when an isolate network can break up in group of two or more networks. Communication between different groups is not possible if there is no connecting help between groups. The situation will become better if different groups can also connect to outer network and communicate with each other using services of external network.
The scenarios represented in situation 1 and 2 can be resolved with use of 4G concept. As 4G gives the concept of convergence, it is possible to connect MANET to outer world with 4G and also communication between different isolated MANET subgroups can be established using concept of 4G.

FACTORS INFLUENCING IMPLEMENTATION OF MANET IN COMMERCIAL ENVIRONMENT: SECURITY ATTACKS IN MANET

The different characteristics of attacks into two main categories [5]: Active and Passive. In passive attacks, attackers are typically camouflaged, i.e. hidden, and tap the communication lines to collect data. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Several papers have presented the security attacks in MOBILE ADHOC [6][7][8][9][10].
<table>
<thead>
<tr>
<th>Technique</th>
<th>Attack</th>
<th>Approach</th>
<th>Implementation</th>
<th>Deficiencies</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techniques for In- trus ion- resistant Ad Hoc Routing Algorithms</td>
<td>DoS</td>
<td>Based on set of techniques: flow-based route access control (flow-based route access control), flow monitoring, source-initiated router switching, fast authentication, referral based resource allocation</td>
<td>Implemented with the existing routing protocol.</td>
<td>1. In the path failure a compromised node could not be identified. 2. Flow status message can cause additional traffic. 3. Implementation did not explained by author.</td>
<td>2003</td>
</tr>
<tr>
<td>Rushing Attack Prevention (RAP)</td>
<td>DoS (rushing attack)</td>
<td>Based on three technique: 1. Secure neighbor detection, 2. Secure route delegation 3. Randomized route request forwarding</td>
<td>Integrated with AODV or DSR.</td>
<td>1. It defends against special type of rushing attack. 2. It incurs higher overhead than other route discovery.</td>
<td>2003</td>
</tr>
<tr>
<td>Best effort Fault Tolerant Routing algo- rithm (BFTR)</td>
<td>Dropping, corruption, misrouting, tampering, delaying, fabrication and replaying</td>
<td>The criterion used is: end-to-end performance measured using the data packet transmission ratio and acknowledgement</td>
<td>Undefined</td>
<td>It will not perform well when misbehaving nodes are increased and when network become heavy loaded</td>
<td>2004</td>
</tr>
<tr>
<td>Based on Attack Detection &amp; Location</td>
<td>Flooding attacks</td>
<td>1. Suggest a resource allocation mechanism (RAM): depends on taking advantage of existing application capability to handle intruders. 2. Uses wireless ad hoc routing and wireless GRID computing and based on managing a multi trust levels in a real time</td>
<td>(RAM) implemented with the wireless router through a suggested component</td>
<td>Undefined</td>
<td>2005</td>
</tr>
<tr>
<td>Mechanism by Geng</td>
<td>DoS</td>
<td>1. New routing mechanism based on common neighbor listening. 2. Each node has a trust value increases quickly and decreases slowly depending on its behavior. 3. Bigger trust value = higher priority to listen.</td>
<td>Implemented in nodes.</td>
<td>If all the common neighbors are under the threshold value of being trusted then there will be no trusted route to the destination.</td>
<td>2006</td>
</tr>
<tr>
<td>Scheme by Lima</td>
<td>DoS</td>
<td>1. Residual path lifetime. 2. Full link lifetime.</td>
<td>In low mobility environment the performance degrades significantly.</td>
<td></td>
<td>2006</td>
</tr>
<tr>
<td>Approach by Dabideen</td>
<td>DoS</td>
<td>1. Based on end-to-end verification and path diversity. 2. Uses digital signature and hash chain. 3. Detects attack by using end-to-end delay and feedback on the number of data packet.</td>
<td>Applied to secure routing through diversity and verification (SRDV) protocol.</td>
<td>Undefined</td>
<td>2009</td>
</tr>
</tbody>
</table>
III. Conclusion

Encrypting wireless links makes it very difficult to share infrastructure. This is a policy issue.

Proposed System Architecture: Preliminary Design

Intrusion Detection System (IDS)

<table>
<thead>
<tr>
<th>IDS activities</th>
<th>Prevention</th>
<th>Intrusion Monitoring</th>
<th>Intrusion Detection</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation</td>
<td>Analysis</td>
<td>Notification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IDS Components

- Protected System
  - Event Generator
  - Set of Events (Logistics, System, Network packets)
  - Audit Trails & Network Monitoring
  - Information Collection Policy
- Database (IDS Configuration)
- Database (IDS Knowledge DB)
- Sensor & Analyze
  - Pattern matching algorithms
- System Information
- Detection Policy
- Attack Response Module
- Response Policy

DOI: 10.9790/0661-1806045158  www.iosrjournals.org  56 | Page
The MANETs provide infrastructure less architecture to mobile-Governance concept, resulting in low cost infrastructure results in MOBILE ADHOC GOVERNANCE concept. This kind of network can achieve constant connectivity and high transmission quality by implementing this concept with 4G, results in the concept of 4GMOBILE ADHOC GOVERNANCE. These kinds of networks will result in real-time information delivery revolution to serve highly mobile service user in m-Governance. The Mobile Ad-hoc Governance must face various technical challenges before its adoption; therefore factors influencing the adoption of MANET in commercial environment must be given proper attention.

References


AUTHOR PROFILE
Chilakalapudi Meher Babu did his M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh (INDIA) and pursuing Ph.D in R.T.M. Nagpur University, Nagpur(India), Currently pursuing Ph.D in the Post-Graduate Teaching Department of Electronics & Computer Science Dept, R.T.M. Nagpur University, Nagpur, India. He has 12 National and International Journal Publications to his credit. His area of interest in research includes MANET, Network Intrusion Detection System on Wireless

DOI: 10.9790/0661-1806045158 www.ijsrjournals.org
Lan’s, IP Address, Routing Algorithms etc.,
Dr. Ashish B. Sasankar did his MCA, M.Tech (CSE), M.Phil. (Computer Science) & Ph.D. in Computer Science from R.T.M. Nagpur University (India). He has a rich experience of 16 years in the field of Education. Currently, he is the Head of the Department of MCA in the most prestigious G.H. Raisoni Institute of Information Technology [GHRIT], Nagpur [India]. He is a Ph.D Guide for Computer Science in the Faculty of Science in R.T.M. Nagpur University, Nagpur (India) and guiding many of his research scholars doing their Ph.Ds in Computer Science in R.T.M. Nagpur University, Nagpur. He has 40 National & International Journal Publications to his credit. He is a Member of the IEEE and CSI.