FALSE DATA DETECTION IN MOBILE AD-HOC NETWORK BASED ON
DIGITAL SIGNATURE

BABAK EMAMI ABARGHOUEI

A project submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013
I dedicated this thesis to my beloved Mother  For her endless support and encouragement
ACKNOWLEDGEMENT

IN THE NAME OF GOD, MOST GRACIOUS, MOST COMPASSIONATE

I would like to acknowledge my supervisor, Dr.Ismail Fauzi bin Isnin, for his support, encouragement, guidance, astute and expert editing. I would like to express gratitude for his patience, generosity, and collaboration.

My lovely family; thank you for your perpetual encouragement and support. Your unwavering love that have shaped my mind and opened the doors of opportunity leading me to become the person I am today.

I would like to thank all of the individuals who have helped me during my thesis study.
ABSTRACT

Routing misbehavior and false communication on wireless sensor network are so significant. An attacker can devour the sensor resources. No central monitoring system, lead to mobile sensor network suffering false communication. This thesis, organized to introduce a new detection method to mitigate the effect of false data on the mobile AD-HOC network. DNACK, which proposed in this thesis, is a new modification of NACK method. DNACK also consider about negative acknowledgment to find the false route messages. DNACK can detect modified messages in the middle of a route in oppose of NACK which, can detect false modified data on the destination. By comparison, the Delivery percentage on NACK and DNACK, DNACK shown better results in opposed to NACK method. Simulation has been done in three modes of node’s mobility Speed in meter per second (M:0, M:5 and M: 10). In all situations, the efficiency of DNACK is better than NACK because in NACK nodes all packets (original and modified) are delivering to destination by contrast in DNACK just original packets are deliver to destination. However the Delivery percentage in NACK is Higher than DNACK which is around 2% for 10 meters per second nodes’ movement. Nevertheless DNACK is more efficient than NACK. On M=10 (m/s) DNACK shown 64% verified messages on Destination in opposed by 60% verified messages on NACK method. In overall the efficiency of packet delivery can be calculated by multiplication of overall delivery by verified packet shows that DNACK method has 51.5 % verified messages delivery in opposed of NACK by 49.8 % delivery on M=10 m/s.
ABSTRAK

Salah laku routing dan komunikasi palsu pada rangkaian pengesan tanpa wayar amat ketara. Penyerang boleh mengambil sumber-sumber pengesan tersebut. Ketiadaan pusat sistem pemantauan, boleh membawa kepada rangkaian pengesan mudah-alih mengalami komunikasi palsu. Kajian ini dijalankan untuk memperkenalkan suatu kaedah pengesanan yang baru untuk mengurangkan kesan data palsu pada rangkaian mudah-alih AD-HOC. DNACK, yang dicadangkan dalam kajian ini, adalah pengubahsuaian baru pada kaedah NACK. DNACK juga mempertimbangkan tentang pengakuan negatif untuk mencari laluan mesej-mesej palsu. DNACK boleh mengesakan mesej-mesej yang telah diubahsuai semasa ia dalam laluan, manakala NACK boleh mengesakan data yang telah diubahsuai pada destinasi. Secara perbandingan, peratus penghantaran pada NACK dan DNACK, DNACK menunjukkan keputusan yang lebih baik berbanding dengan kaedah NACK. Simulasi telah dijalankan pada 3 mod pergerakan kelajuan nod-nod dalam meter sesaat (M:0, M:5 and M:10). Dalam semua situasi, keberkesanan DNACK adalah lebih baik dari NACK kerana dalam NACK kesemua paket-pakes nod (yang asal dan diubahsuai) dihantar kepada destinasi sementara DNACK hanya menghantar paket-paket yang asli kepada destinasi. Walau bagaimanapun, peratus penghantaran NACK adalah lebih tinggi daripada DNACK iaitu dalam sekitar 2% untuk 10 meter sesaat pergerakan nod-nod. Namun DNACK mempunyai kecekapan yang lebih baik dari NACK. Pada M=10 (m/s) DNACK memperoleh 64% mesej-mesej yang disahkan pada destinasi manakala hanya 60% mesej-mesej yang disahkan dengan menggunakan kaedah NACK. Secara keseluruhan, kecekapan penghantaran paket boleh dikira dengan membuat pendaraban keseluruhan penghantaran oleh paket yang disahkan menunjukkan bahawa kaedah DNACK mempunyai peratus penghantaran mesej-mesej yang disahkan 51.5% manakala NACK mempunyai 49.8% penghantaran pada M=10 m/s.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF FIGURE</td>
<td></td>
<td>xii</td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 Introduction 1

1.1.1 Manet Characteristics 2

1.2 Background of The Study 3

1.2.1 Manet Routing Protocol 3

1.2.2 Manet Security Goal 4

1.2.3 Background of Problem 5

1.3 Statement of Problem 8

1.4 Purpose of The Study 8

1.5 Objectives of The Study 9

1.6 Research Questions 10

1.7 Significance Of The Study 10

1.8 Scope of The Study 11

## 2 LITERATURE REVIEW

2.1 Introduction 14
# 2.2 False Data Definition

- 2.2.1 Original Data In False Route
- 2.2.2 False Data In Original Path (Modified Data)

# 2.3 Brief Views of False Data

# 2.4 Summarizes Secure Architecture Method

- 2.4.1 Manet Security Threat
- 2.4.2 Attack Classification
  - 2.4.2.1 Classification Based on The Mode Of Attack
  - 2.4.2.2 Classification Based on The Origin Of Attack
- 2.4.3 Attacks Against The Routing Protocols

# 2.5 Current Security Solution Method

- 2.5.1 A Security Solution Based on Cryptography Method
- 2.5.2 Security Solutions Based on Routing Method
- 2.5.3 Credit-Based Scheme Security Solution
- 2.5.4 Reputation-Based Scheme Security Solution
- 2.5.5 En-Route Filtering Security Solution
  - 2.5.5.1 Secure Ticket-Based En-Route Filtering (Stef)
  - 2.5.5.2 An Interleaved Hop-By-Hop Authentication Scheme (Iha)
  - 2.5.5.3 Dynamic En-Route Filtering (Def) Scheme
  - 2.5.5.4 Commutative Cipher Based En-Route Filtering (Ccef)
  - 2.5.5.5 Location-Based Resilient Security (Lbrs) Scheme
  - 2.5.5.6 Virtual Energy-Based Encryption And Keying For Wireless Sensor Network
  - 2.5.5.7 A Bandwidth-Efficient Cooperative Authentication (Becan) Scheme
  - 2.5.5.8 Analysis About En-Route Filtering Schemes

# 2.6 Conclusion

## 3 RESEARCH METHODOLOGY

- 3.1 Introduction
- 3.2 Operational Framework
- 3.3 Literature Review
- 3.4 Problem Formulation
- 3.5 Implementation And Network Design
3.5.1 Implementation The Nack Method As I-Nack 46
3.5.2 Designing Dnack Due To Thesis Goal 47
3.5.3 Implementation The Dnack Method 47
3.6 Simulate The Protocols 47
3.7 Finding And Compare The Results 48
3.8 Summarizing And Writing Up The Project Document 48
3.9 Justification Of Using Simulation 48
3.10 Simulation Tool 48
3.11 Evaluation Metrics 49
  3.11.1 PDR, Packet Delivery Percentage 49
  3.11.2 NDP, Node Delay Processing Time 50
  3.11.3 Network Throughput 50
  3.11.4 False Packet Delivery Percentage 50
  3.11.5 Verified Packet Delivery Percentage 50
3.12 Chapter Summary 51

4 DESIGN AND DEVELOPMENT

4.1 Introduction 52
4.2 NACK Characteristic 52
  4.2.1 Negative Acknowledgment Methodology 52
  4.2.2 NACK Methodology 53
  4.2.2.1 NACK Assumption 53
  4.2.3 NACK Communication Method 54
4.3 The D/NACK Algorithm 56
4.4 Security Architecture 57
4.5 Digital Signature Algorithm In MANET 58
  4.5.1 RSA/ DSA Methodology 59
4.6 Digital Signature Based on RSA Nature 62
4.7 Conclusion 63

5 IMPLEMENTATION AND SIMULATION RESULTS

5.1 Introduction 64
5.2 Nack Parameter 65
5.2 Implementation 66
5.3 Evaluation Part 67
6  CONCLUSION

6.1 Introduction 86
6.2 Overview Of The Study 86
6.3 Project Achievement 87
6.4 Limitation Of The Project 88
6.5 Recommendation 88

REFERENCES 89
<p>|| TABLE NO. | TITLE | PAGE |
|---|---|---|
| 2.1 | Performance analysis of en-route filtering schemes | 38 |
| 2.2 | Summary of various en-route filtering schemes for wireless sensor networks | 39 |
| 4.1 | Reduction algorithm for RSA | 60 |
| 5.1 | Nack notations (sun, chen et al. 2012) | 65 |
| 5.2 | Nack configuration table | 67 |
| 5.3 | Dnack configuration | 71 |
| 5.4 | Comparison reading time in end hop | 75 |
| 5.5 | Communication between two neighbors by rsa signature | 77 |</p>
<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>False data on false route</td>
<td>16</td>
</tr>
<tr>
<td>2.2</td>
<td>False data in original path (modified data)</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Classification of security attacks in manet</td>
<td>19</td>
</tr>
<tr>
<td>2.4</td>
<td>Mac authentication schema</td>
<td>31</td>
</tr>
<tr>
<td>3.1</td>
<td>Researches operational framework</td>
<td>43</td>
</tr>
<tr>
<td>3.2</td>
<td>Proposed schema design framework</td>
<td>44</td>
</tr>
<tr>
<td>4.1</td>
<td>Nack communications schema</td>
<td>55</td>
</tr>
<tr>
<td>4.2</td>
<td>Function recv(p,h) of class tcpagent (issariyakul 2012).</td>
<td>56</td>
</tr>
<tr>
<td>4.3</td>
<td>Nack packet verification schema</td>
<td>59</td>
</tr>
<tr>
<td>4.4</td>
<td>Shows the signature verification schema in nack chain.</td>
<td>62</td>
</tr>
<tr>
<td>4.5</td>
<td>Dsa nature.</td>
<td>62</td>
</tr>
<tr>
<td>5.1</td>
<td>Adversaries percentage impact of dropping packet. (sun, chen et al. 2012)</td>
<td>68</td>
</tr>
<tr>
<td>5.2</td>
<td>Routing overhead (sun, chen et al. 2012)</td>
<td>69</td>
</tr>
<tr>
<td>5.3</td>
<td>Random position /destination diagram</td>
<td>72</td>
</tr>
<tr>
<td>5.4</td>
<td>Packet delivery under dropping attack</td>
<td>73</td>
</tr>
<tr>
<td>5.5</td>
<td>Averages of nodes delay time per communication</td>
<td>78</td>
</tr>
<tr>
<td>5.6</td>
<td>Comparison of delivery and efficiency dnack</td>
<td>79</td>
</tr>
<tr>
<td>5.7</td>
<td>Comparison of delivery and efficiency nack</td>
<td>80</td>
</tr>
<tr>
<td>5.8</td>
<td>Comparisons of delivery and efficiency dnack vs nack in same attack same mobility</td>
<td>81</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.9</td>
<td>Throughput comparison between nack and dnack</td>
<td>83</td>
</tr>
<tr>
<td>5.10</td>
<td>Node delay comparison in nack /dnack and efficiency of dnack / nack</td>
<td>84</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

MANET or Mobile AD-HOC Network is a wireless system that embraces mobile nodes. It is generally denoted to a decentralized autonomous system. MANET does not require any fixed infrastructure such as base stations, router, infrastructure, and therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously to environments such as military battlefields and rescue operations.

Mobile nodes consist of mobile devices as well as mobile phone, laptop, home computer, MP3 player, PDA or personal digital assistant. Mobile Nodes can be applied in a variety of gadgets, such as ships, airplanes, or land, irrespective of their location as they can participate in communication. Decentralized autonomous feature leads to MANET to have some special feature such as self-connectivity and easy deployment. These features of MANETs make it the best candidate in challenging situations such as emergency, surveillance and rescue operations.

However those characteristic make MANET as so interesting object of communication but also having no central monitoring system, fixed infrastructure and nodes self-configuration lead to confidential or secure communication on Mobile nodes faced by high cost.
GCSs or secure group communication systems required a confident secure architecture. Due to special characteristic MANET Security faced by some technical challenges such as “resource-constrained environments (e.g., Bandwidth, memory size, battery life, and computational power), openness to eavesdropping and security threats, unreliable communication, no infrastructure support, and rapid changes in network topology due to user mobility which could cause group merge/partition events to occur dynamically”(Cho and Chen 2011). MANET Nodes’ mobility is the most specific characteristic in whole AD-HOC Network domain.

1.1.1 MANET Characteristics

A. **Dynamic network topology**: because of nodes’ mobility, network structure modified constantly. Network domain may have different cluster or zone, according to nodes’ motivation, a node might be left its zone and joined to another zone or even joined to one another network.

B. **Energy constrained nodes**: due to nodes’ mobility, MANET need to have embedded low power instead of direct power, Manet’s nodes will most often rely on batteries as their power source. Because of this limitation AD-HOC nodes cannot support the heavy computing algorithm

C. **Bandwidth’s restriction**: low power nodes and low power computing leads to Mobile nodes face by some limitation on bandwidth. This may effect on the number and messages’ size during communication.

D. **Lack of physical security**: fading the central physical monitoring system because of Nodes’ motion ability leads to exposure of the network nodes increase the possibility of attacks against the network. Owing to nodes’ mobility, the risk of physically compromised/tampering by ID spoofing and so forth is bigger than outmoded network nodes.
1.2 Background of the Study

Considering to MANET characteristic, vast of majority researches have been proposed to solve MANET security challenge such as routing protocols, secure routing protocols, trusted base party and so forth. Dynamic routing protocol limitation has been covered by different routing protocol, can be introduced into a majority of routing link-state and distance vector.

1.2.1 MANET Routing Protocol

MANET gradually exploited the wireless communication world as the common means of human communication. Devices are configured with Wi-Fi cards as hotspots in many places such as universities, offices, airports, and hotels. It stood as a major source of communication in this modern world. This challenged the researchers around the world to enforce their research in developing MANET. In such advanced communication network, routing protocol plays a key role, as it is one of the major aspects to route the data in a network. Many researchers have proposed different protocols.

MANET routing protocol noticed experimental Request For Comments (RFC) since 2003. Implementation and deployment of the protocols have not properly addressed by RFCs, but the routing protocol algorithms proposed were identified as trial technology with the high probability that will result into a standard. Enormous research work has been focused on different routing protocols such as Dynamic Source Routing (DSR), Optimized Link State routing (OLSR), Temporarily Ordered Routing Algorithm (TORA) and Ad hoc On-demand Distance Vector (AODV), for their development and standardization of routing support from MANET Working group (WG) of Internet Engineering Task Force (IETF) (Luo, Ye et al. 2009). The aim of proposing the variety of routing protocols in different shape there was nothing else to except approaching the high level of network security.
Secure mobile network necessities like privacy, authentication, integrity and non-repudiation rely on a secure key management framework. (Bala Krishna and Doja 2011)

1.2.2 MANET Security Goal

A. **Confidentiality** makes sure that the transmitted data packet is not being exposed to unauthorized users.

B. **Availability** makes sure that the resource will be available to trusted party and unavailable to unauthorized.

C. **Integrity** confirms that data is not being corrupted or tampered with during transmission. Integrity encompasses data integrity and origin integrity. Data integrity ensures that original content of the data is not altered or tampered with. Origin integrity verifies the sender’s identity and ensures that the data has been sent by the appropriate entity.

D. **Authenticity** verifies that a user is permitted or has the proper permission to access or use a resource.

E. **Non-Repudiation** binds a user’s identity with his/her action, so that the user cannot deny the action he has performed.

Owing to these goals, communication had to reach the highest level of security that even trusted party cannot understand the communication of its neighborhood. According to networks’ confidentiality and integrity, there are vast of majority research have been focused only on misbehavior detection.

In summary, security is a most important part of communication. It cannot be reach to high level of security if even one part of security goal going to neglect. MANET is so interesting to every part of communication as well as the battlefield, medical sensors, body sensor, desert and ocean telecommunication and so forth by considering to C.I.A. The MANET security architecture had to cover each main part, Confidentiality, Integrity and Availability.
1.2.3 Background of Problem

MANET or Mobile AD-HOC network is composed of an small countable mobile nodes having limited resource such as computation capacity, memory space, low power/computing and low Bandwidth communication. Mobile nodes treated to deployed in hostile environment. In such situation mobile nodes will engaged to variety of attacks for instance false data, masquerade, selective forwarding, eavesdropping and so forth. Attacker can rise up number of attacks from outside as well as inside zone. There are a number of security framework have been proposing to isolate the Mobile nodes in oppose of malicious nodes.

Due to MANET characteristic, there are different kinds of attack in mobile network layers. Table 2.1 contains of some information of common attack on MANET layers. By comparing between those kinds of attacks, false data injection or false communication attack is much more significant. Considering to false data nature, it can cover the variety of routing attacks such as wormhole, false route and modified data. The definition of false data has been discussed in section 2.2.

In a MANET, since all communications are totally exposed and disposed to be captured, an efficient encryption system can be provided the secure communication. Due to MANET limitation such as energy, low power, low power computing, and lack of centralized infrastructure, cryptography method is recommended significantly to prevent of external attack (Bala Krishna and Doja 2011). But on the other hand crypto system need powerful algorithm and need more power and energy as well, considering to route path and intermediate nodes, misbehavior acting and false data injection detectable by routing table, much easier than using the crypto system as well as symmetric or Asymmetric methods (Su 2010).

Due to False data attack, there are two basic methods to detect such this kind of attack: en-route filtering and end-to-end detection based on cryptography method. Table 2.2 shown the summarize of false data detection. By comparison, those ideas false data can be controlled by cooperation between these two classes. NACK
method is the en-route monitoring method which, proposed by (Sun, Chen et al. 2012). NACK nodes also are engaged by Digital signature method to detect the modified data in end-to-end path. NACK is significant method which in this thesis tried to simulate this method to detect the false data.

End-to-end detection has been supported by variety researchers considering to MANET limitation, and nature of false data which lets off the attacker to saturate the network Bandwidth. In (CPNS), or Cyber-Physical Networked Systems, unauthorized node could inject false data for controlling through the MANET nodes, which not only threaten on confidentially and integrity of data, but also false data can be lead to consumes the CPU and node power and having action as well as DOS, or Denial Of Service attack by threatening the network availability(Xinyu, Jie et al. 2012).

Due to mobile nodes limitation, hop-by-hop detection can be much more significant than end-to-end. According to those proposed method for false data detection, by engaging the en-route monitoring method and crypto system together, we can have the much more efficient method for detecting this kind of attack.

Sensor nodes sense the events that occur in their surrounding environment. Generate event report for the sensed information and the event report has to be send to the base station through the en-route nodes. When event report is forwarded through en-route node a compromised node can forge the report. False data contain false information from compromised nodes. This false data injection attack depletes the energy of the en-route nodes. This may be dangerous in scenarios such as battlefield surveillance and environmental monitoring by making false decision. Moreover, it is a difficult task to monitor all the sensor nodes in the field of interest.

However, several recent research efforts have proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions can prevent false reports injection by outside attackers. They are made ineffective when any single node is compromised. One solution to reduce the impact of false
Data injection into the network through a compromised node is to filter the false data by the en-route node as early as possible before reaching the base station. Authentic and accurate data is provided to surrounding sensor node and to the sink through en-route filtering scheme. En-route filtering is an effective way to defeat false data injection attacks. Moreover Messages’ authenticity will be check by intermediate nodes as well as destination on en-route filtering methods. Due to this nodes activity the false messages will not be able travelling more and the nodes resources will be survived. This paper describes about many of the existing en-route filtering schemes. In addition analyze about the advantages and disadvantages of the related en-route filtering scheme.

According to previous research in FDD, or False Data Detection, most of them have the same consumption to detect the false data and misbehavior action based on hop-by-hop authentication (Azer, El-Kassas et al. 2008; Su 2010; Abdalla, Saroit et al. 2011; Gupta, Kar et al. 2011).

In (CPNS) or Cyber-Physical Networked Systems, unauthorized node could inject false data for controlling through the MANET nodes, which not only threaten on confidentiality and integrity of data, but also false data can be lead to consumes the CPU and node power and having action as well as DOS, or Denial Of Service attack by threatening the network availability.

A number of en-route filtering methods have been proposing To contract with this issue (Xinyu, Jie et al. 2012). As can be seen there are a number of previous research which focusing on localization nodes in different security methods.

Due significance of the false data, by deep exploration on more than 80 papers on variety method we find NACK (Sun, Chen et al. 2012) method which so interesting method. NACK member no need to have any extra devices and NACK member can detect false data in the false route so easily. Nevertheless, because of NACK methodology, members can detect the false modified data in end-to-end detection. Due to this
NACK characteristic, we proposed the new method of NACK to improved NACK efficiency while network faced by man in a middle and fabrication messages. DNACK can be detected fabricated message Due to hop-by-hop message authentication.

1.3 Statement of Problem

False communication on wireless sensor network not only absorbed the node's resources also, it can be break down a network such as denial of service attack. The false reports consume lots of network and computation resources and shorten the lifetime of sensor networks. Hence, to ensure the normal operation of the system, it is critical to filter false data at forwarding nodes before arriving at the destination (Jeba and Paramasivan 2012).

Though several recent research efforts have, proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions mostly considered about false reports or false route messages. In addition, there are countable methods, they are considered about false modified data. According to false data nature, having a security method to detect the false data in false route and modified data by cooperation of intermediate nodes still a challenging problem.

1.4 Purpose of the Study

Due to MANET limitation, mobile nodes will be faced by extra cost of communication while sending the false data to destination. False data not only absorbed the nodes energy moreover, it can be broken down a network such as denial of service attack. The false reports consume lots of network and computation resources and shorten the lifetime of sensor networks. Hence, to ensure the normal
operation of the system, it is critical to filter false data at forwarding nodes before arriving at the destination (Jeba and Paramasivan 2012).

In this thesis, we aimed to utilize the Digital signature algorithm by (NACK) negative acknowledgment method to detect false data in a false route and false injected data with intermediate nodes. DNACK is the modified NACK method which can detect false data in a false route and also false data injected by an attacker in the communication chain.

The aim of this project is to identify the weakness, strength, and the efficiency of en-route filtering on Mobile networks. DNACK can be introduced as a good candidate in Risky situations, while the probability of a man-in-the-middle or packet fabrication is high. DNACK also can be presented on a battlefield while the messages’ missions need to have a high degree of confidentiality. DNACK method has been discussed deeply in Chapter 4 and the results of DNACK method are shown in Chapter 5 based on packet delivery percentage and false data detection’s time.

1.5 Objectives of the Study

MANET is a type of multi-hop network, infrastructure-less and the most important self-organizing. Due to its wireless and distributed nature, there is a great challenge for system security designers. In the last few years, security problems in MANETs have attracted much attention; most of the research effort focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or False Data Detection and response.

According to the last researches in MANET FDD that mentioned in Chapter 2, objectives of this research can be partitioned to 3 parts as well as:

1) Study on the existing False Data Detection method on MANET.
2) Implement and develop the most significant detection method. In this thesis the “negative acknowledgment,” (NACK) method has been chosen as a main method.
3) Propose the new enhancement of NACK called DNACK.
4) Compare the efficiency of the proposing method (DNACK) in comparison by chosen the method (NACK) (Sun, Chen et al. 2012).

1.6 Research Questions

A. How messages integrity can be guaranteed in hop-by-hop monitoring system?
B. What are the challenges of the NACK method for false data Detection in MANET?
C. How to enhance the NACK method for having the more confidential communication chins?

1.7 Significance of the Study

This research done, based on the issues of en-route monitoring in 802.11, proposing an optimized technique for reducing mentioned issues. This proposed technique is able to prepare a mobile network environment away from false data threats. The findings of this research are important to enhance the messages’ confidentiality by engaging the digital signature in NACK method.

DNACK can be introduced as a good candidate on Risky situation, while the probability of a man in a middle or packet fabrication is high. DNACK also can be presented on Battlefield while the messages’ missions need to have a high degree of confidentiality. DNACK method has been discussed deeply in chapter 4 and the
results of DNACK method are shown in chapter 5 based on packet delivery percentage and false data detection’s time.

1.8 Scope of the Study

This report tries to have a brief illustration on security threats and challenges of false data injection in MANET. There are two main parts of this thesis, in the first part previous research in false data Detection are discussed .Implementation in NS-2.35 would be the second part of this thesis .Result of implementation are compared with the result of existing research in false data detection were proposed by(Sun, Chen et al. 2012).

The scope of this project is limited to the following

1. The NACK method on DSR routing protocols
2. Using Digital signature algorithm for Messages authentication and verification
3. Efficiency of NACK and DNACK routing method in mobile network
4. The simulation environment will be based on Network Simulator-2(NS-2.35).
5. The evaluations between this two method (NACK and DNACK) based on nodes Delay process, packet delivery ratio, and successful data delivery.
REFERENCES


