Identification of Misbehaviour and Packet Loss Activities in Mobile Adhoc Network

G. Malathi  
Assistant Professor, Department of Computer Science and Engineering, Thangavelu Engineering College, Chennai, India

Abstract: In the existing system security was lack in MANET. Because of the Open medium and distribution of the nodes in various locations, makes MANET vulnerable to malicious to attackers. Now, the data is send to the Destination Node via intermediate nodes in the Encrypted format. Each node has to pass the Acknowledgement after the Receiving of the data. If any of the nodes didn’t pass the Acknowledgement, then the Source Node will send the data to the Destination via another Route. Then the MRA is filed. If the Destination Claims Duplication of the Data, then Source will find the Misbehavior. If there is no Data, then resend the Data is stored in the Destination, again the packet dropped node is considered as attacker, and then the node is removed from the network. We can Process, the server will identify the buffer level of the intermediate nodes. If the packets are dropped due to inadequate of Space/memory then the node is not considered as an attacker.

Keywords: Mobile Adhoc Network.

1. Introduction

A. Domain specification

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves:

- Mobile communication
- Mobile hardware
- Mobile software

B. Need

Mobile communication

The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as Protocols, Services, Bandwidth, and Portals necessary to facilitate and support of the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems which offer the same service. Since the media is unguided/unbounded, the overlaying infrastructure is more of radio wave oriented. That is, the signals are carried over the air to intended devices that are capable of receiving and sending similar kinds signals.

Mobile hardware

In mobile computing mobile hardware includes mobile devices or mobile components

Mobile software

Mobile Software deals with the characteristics and requirements of mobile applications.

Fig. 1. Mobile communication

C. Scope

The main motive of this project is to identify the misbehavior and packet loss activities in mobile ad hoc networks.

2. Literature review


An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q.
An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host’s wireless transmissions. This paper presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates. For all but the highest rates of host movement simulated, the overhead of the protocol is quite low, falling to just 1% of total data packets transmitted for moderate movement rates in a network of 24 mobile hosts. In all cases, the difference in length between the routes used and the optimal route lengths is negligible, and in most cases, route lengths are on average within a factor of 1.01 of optimal.

Ad hoc wireless networks are defined as the category of wireless networks that utilizes multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure hence, they are called infrastructure less networks. The lack of any central coordination makes them more vulnerable to attacks than wired networks. Due to some unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure therefore, detection should be added as another defense before an attacker can breach the system. Network intrusion detection is the process of monitoring the events occurring in the network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality. In this paper, we define and discuss various techniques of Intrusion Detection. We also present a description of routing protocols and types of security attacks possible in the network.

An ad hoc network is a group of wireless mobile computers (or nodes), in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. In this paper, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

3. System analysis

A. Existing system

In the Existing system, the security was low in the Mobile Ad-hoc Networks. Also the due to open source nature and remote distribution of the nodes, the nodes can be used for vulnerable purposes.

- For example, due to the nodes’ lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks.
- In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network.
- Furthermore, because of MANET’s distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs.

Disadvantages:

- Less security so that the attackers can easily hack the data.
- Unable to find that the data was originally hacked by the hacker/attacker, because sometimes the data loss can happen due to node low buffer level.

B. Proposed system

In the Proposed System, to overcome the drawbacks of the existing system, we are introducing a new Intrusion Detection System called EAACK.

- If a Source wants to send the data to the Destination via intermediate nodes, each node have to send the Acknowledgement to the previous node.
- If the packet is received by the Destination, then we can conclude that the data is safelyreached to Destination node via alternate path. Also a MisReport Authentication (MRA) will be filed.
- Once receiving the data, the destination node check the data in its history, if the data is present then we can conclude that the node which lied that they didn’t received the data. Else we can conclude that the node have lost the data packets.
- Once the attacker is identified, they will be removed from the network. Also for security purpose we can encrypt the data packet during transmission.

C. Modification

The data can also be lost due to the Low Buffer level of the node. So we are also calculating the Buffer Level of each node. By calculating the buffer level we can identify whether it is
normal data loss or data loss due compromise of the node. 

Advantages:

- Security level will be increased due to the Encrypting the data packet, also that the acknowledgment from each node will denote that the data packets are send safely.
- We can also identify that the packet loss can occur due to the low buffer level problem.

4. System specification

Introduction

The requirement specification is a technical specification of requirement for the software products. It is the first step in the requirement analysis process it lists the requirement of a particular software system including functional performance and security requirements. This describes the project target audience and its user interface hardware and software requirement

A. Software requirements
- Platform : Windows XP
- Front End : .NET
- Back End : SQL Server

B. Hardware requirements
- Processor : Pentium IV
- RAM : 512 MB
- HDD : 80 GB

5. Project description

A. Project definition

Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi-hop.

In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery.

B. Module description

The 5 major modules are
- Network construction
- Data transmission and acknowledge retrieval
- Detection of packet loss
- Misbehaviour report
- Identify and removal the attacker

1) Network construction

To implement the Project concept, first we have to construct a network which consists of ‘n’ number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. To show this concept we’ll create the Node frame which contains the time. Based on the time change we can assume that the nodes are moving across the network. For each node we have to create a Node Frame which contains the Node information. Destination Node field to transfer the data and the browse button to upload the data from Node’s directory.

2) Data transmission and acknowledge retrieval

Once we created node in the Network, any of the node can send to the other nodes. To send the data to the destination node, the Source node will choose the node information from the nodes list and upload the data from its directory and transmit the data via intermediate node. Once the intermediate node receives the data packets, they have to send the Acknowledgement to the Source node. Based on the acknowledgement from the intermediate nodes, the Source node can infer that the packet is transmitting to the destination node.

3) Detection of packet loss

As per our concept, while the data is travelling across the network it possible for any of the nodes can drop the packets or node can lie that they haven’t received the acknowledgement for data packets that they have received. So that we can conclude that any of two node is performing malicious activity. To identify the data Malicious Node in the Network, we are filing the Misbehaviour Report Authentication.

4) Misbehaviour report

Once we identify the malicious activity has occurred in the network, the network will file the Misbehaviour Report Authentication on the two nodes. Once the Misbehaviour Report Authentication is filed, then the Source node will send the data packets to the destination node via alternate path. The Destination node will check with its directory and if the same data packets are already been received then it will intimate same to the nodes. So that we can conclude that the node which lied is considered as Malicious Node. Otherwise packet lost node is considered as Malicious Node.

5) Identify and removal the attacker

The data loss can occur due the node instability. So that we
can say that the data packet loss has occurred due to more number of data packets are transferred than its Buffer Level. Due to the importance of this concept we are extending our project, by identifying the data loss is occurred whether by node instability or Malicious Activity. For this purpose, we can maintain the buffer level for each intermediate node, so that we can conclude the data loss is a Genuine Loss or Attacker Packet loss. If it is attacker packet loss, we can remove the attacker from the Network. So that we can secure our Network from Intrusions.

6) Algorithm used

Encryption basics
- Encryption is yet another process by which information is protected from unauthorized access.
- It is normally accomplished by rendering the original information unreadable by using a reversible technique known only to the authorized entities.
- A symmetric key encryption algo. Invented by Ron Rivest.
- Normally uses 64 bit and 128 bit key sizes.
- Most popular implementation is in WEP for 802.11 wireless networks and in SSL.
- Cryptographically very strong yet very easy to implement.
- Consists of 2 parts: Key Scheduling Algorithm (KSA) & Pseudo-Random Generation Algorithm

Array initialization
C Code:
```c
char S[256];
int i;
For(i=0; i< 256; i++)
S[i] = i;
```
After this the array would like this:
```plaintext
S[] = { 0,1,2,3, ……, 254, 255 }
```
The initialized array S[256] is now run through the KSA. The KSA uses the secret key to scramble the array.

Encryption using RC4
- Choose a secret key
- Run the KSA and PRGA using the key to generate a keystream.
- XOR keystream with the data to generate encrypted stream.
- Transmit Encrypted stream.

Description using RC4
- Use the same secret key as during the encryption phase.
- Generate keystream by running the KSA and PRGA.
- XOR keystream with the encrypted text to generate the plain text.

Making of a RC4 File Encryptor
- Using a secret key generate the RC4 keystream using the KSA and PRGA.
- Read the file and xor each byte of the file with the corresponding keystream byte.
- Write this encrypted output to a file.
- Transmit file over an insecure channel.

6. System design

A. Architecture diagram

1) Collaboration diagram

Another type of interaction diagram is the collaboration diagram. A collaboration diagram represents a collaboration, which is a set of objects related in a particular context, and interaction, which is a set of messages exchange among the objects within the collaboration to achieve a desired outcome.

7. Software specification

A. .NET framework

The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet.

Objectives of .NET framework
1) To provide a consistent object-oriented programming environment whether object codes is stored and executed locally on Internet-distributed, or executed remotely.
2) To provide a code-execution environment to minimizes software deployment and guarantees safe execution of code.
3) Eliminates the performance problems.
4) There are different types of application, such as Windows-based applications and Web-based applications. To make communication on distributed environment to ensure that code be accessed by the .NET Framework can integrate with any other code.

1) Components of .NET framework

The common language runtime (CLR):

The common language runtime is the foundation of the .NET Framework. It manages code at execution time, providing important services such as memory management, thread management, and remoting and also ensures more security and robustness. The concept of code management is a fundamental principle of the runtime. Code that targets the runtime is known as managed code, while code that does not target the runtime is known as unmanaged code.

The .NET framework class library:

It is a comprehensive, object-oriented collection of reusable
types used to develop applications ranging from traditional command-line or graphical user interface (GUI) applications to applications based on the latest innovations provided by ASP.NET, such as Web Forms and XML Web services.

The .NET Framework can be hosted by unmanaged components that load the common language runtime into their processes and initiate the execution of managed code, thereby creating a software environment that can exploit both managed and unmanaged features. The .NET Framework not only provides several runtime hosts, but also supports the development of third-party runtime hosts.

Internet Explorer is an example of an unmanaged application that hosts the runtime (in the form of a MIME type extension). Using Internet Explorer to host the runtime to enables embeds managed components or Windows Forms controls in HTML documents.

Features of the common language runtime

The common language runtime manages memory; thread execution, code execution, code safety verification, compilation, and other system services these are all run on CLR.

- Security
- Robustness
- Productivity
- Performance

Security:

The runtime enforces code access security. The security features of the runtime thus enable legitimate Internet-deployed software to be exceptionally feature rich. With regards to security, managed components are awarded varying degrees of trust, depending on a number of factors that include their origin to perform file-access operations, registry-access operations, or other sensitive functions.

Robustness:

The runtime also enforces code robustness by implementing a strict type- and code-verification infrastructure called the common type system (CTS). The CTS ensures that all managed code is self-describing. The managed environment of the runtime eliminates many common software issues.

Productivity:

The runtime also accelerates developer productivity. For example, programmers can write applications in their development language of choice, yet take full advantage of the runtime, the class library, and components written in other languages by other developers.

Performance:

The runtime is designed to enhance performance. Although the common language runtime provides many standard runtime services, managed code is never interpreted. A feature called just-in-time (JIT) compiling enables all managed code to run in the native machine language of the system on which it is executing. Finally, the runtime can be hosted by high-performance, server-side applications, such as Microsoft® SQL Server™ and Internet Information Services (IIS).

B. ASP.NET

ASP.NET is the next version of Active Server Pages (ASP); it is a unified Web development platform that provides the services necessary for developers to build enterprise-class Web applications. While ASP.NET is largely syntax compatible, it also provides a new programming model and infrastructure for more secure, scalable, and stable applications.

ASP.NET is a compiled, NET-based environment, we can author applications in any .NET compatible language, including Visual Basic .NET, C#, and JScript .NET. Additionally, the entire .NET Framework is available to any ASP.NET application. Developers can easily access the benefits of these technologies, which include the managed common language runtime environment (CLR), type safety, inheritance, and so on.

ASP.NET has been designed to work seamlessly with WYSIWYG HTML editors and other programming tools, including Microsoft Visual Studio .NET. Not only does this make Web development easier, but it also provides all the benefits that these tools have to offer, including a GUI that developers can use to drop server controls onto a Web page and fully integrated debugging support.

Developers can choose from the following two features when creating an ASP.NET application. Web Forms and Web services, or combine these in any way they see fit. Each is supported by the same infrastructure that allows you to use authentication schemes, cache frequently used data, or customize your application’s configuration, to name only a few possibilities.

Web Forms allows us to build powerful forms-based Web pages. When building these pages, we can use ASP.NET server controls to create common UI elements, and program them for common tasks. These controls allow us to rapidly build a Web Form out of reusable built-in or custom components, simplifying the code of a page.

ASP.NET provides easy-to-use application and session-state facilities that are familiar to ASP developers and are readily compatible with all other .NET Framework APIs.

ASP.NET takes advantage of performance enhancements found in the .NET Framework and common language runtime. Additionally, it has been designed to offer significant performance improvements over ASP and other Web development platforms. All ASP.NET code is compiled, rather than interpreted, which allows early binding, strong typing, and just-in-time (JIT) compilation to native code, to name only a few of its benefits. ASP.NET is also easily factorable, meaning that developers can remove modules (a session module, for instance) that are not relevant to the application they are developing.

ASP.NET provides extensive caching services (both built-in services and caching APIs). ASP.NET also ships with performance counters that developers and system administrators can monitor to test new applications and gather metrics on existing applications.

ASP.NET offers the Trace Context class, which allows us to
write custom debug statements to our pages as we develop them. They appear only when you have enabled tracing for a page or entire application. Enabling tracing also appends details about a request to the page, or, if you so specify, to a custom trace viewer that is stored in the root directory of your application.

The .NET Framework and ASP.NET provide default authorization and authentication schemes for Web applications. We can easily remove, add to, or replace these schemes, depending upon the needs of our application.

ASP.NET configuration settings are stored in XML-based files, which are human readable and writable. Each of our applications can have a distinct configuration file and we can extend the configuration scheme to suit our requirements.

C. XML web services:

XML Web services are applications that can receive the requested data using XML over HTTP. XML Web services are not tied to a particular component technology or object-calling convention but it can be accessed by any language, component model, or operating system. In Visual Studio .NET, you can quickly create and include XML Web services using Visual Basic, Visual C#, JScript, Managed Extensions for C++, or ATL Server.

XML support:
Extensible Markup Language (XML) provides a method for describing structured data. XML is a subset of SGML that is optimized for delivery over the Web. The World Wide Web Consortium (W3C) defines XML standards so that structured data will be uniform and independent of applications. Visual Studio .NET fully supports XML, providing the XML Designer to make it easier to edit XML and create XML schemas.

Features of SQL SERVER:

The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services. SQL-SERVER database consist of six type of objects,

They are,
1. TABLE
2. QUERY
3. FORM
4. REPORT
5. MACRO

TABLE:
A database is a collection of data about a specific topic.
Views of table:
We can work with a table in two types,
1. Design View
2. Datasheet View

Design View:
To build or modify the structure of a table we work in the table design view. We can specify what kind of data will be hold.

Datasheet View:
To add, edit or analyses the data itself we work in tables datasheet view mode.

Query:
A query is a question that has to be asked the data. Access gathers data that answers the question from one or more table. The data that make up the answer is either dynast (if you edit it) or a snapshot (it cannot be edited). Each time we run query, we get latest information in the dynast. Access either displays the dynast or snapshot for us to view or perform an action on it, such as deleting or updating.

Forms:
A form is used to view and edit information in the database record by record. A form displays only the information we want to see in the way we want to see it. Forms use the familiar controls such as textboxes and checkboxes. This makes viewing and entering data easy.

Views of Form:
We can work with forms in several primarily there are two views,

They are,
1. Design View
2. Form View

Design View:
To build or modify the structure of a form, we work in forms design view. We can add control to the form that are bound to fields in a table or query, includes textboxes, option buttons, graphs and pictures.

Form View:
The form view which display the whole design of the form.

Report:
A report is used to vies and print information from the database. The report can ground records into many levels and compute totals and average by checking values from many records at once. Also the report is attractive and distinctive because we have control over the size and appearance of it.

Macro:
A macro is a set of actions. Each action in macros does something. Such as opening a form or printing a report. We write macros to automate the common tasks the work easy and save the time.

Module:
Modules are units of code written in access basic language. We can write and use module to automate and customize the database in very sophisticated way.

8. System testing and maintenance

A. Testing
Testing is a set of activities that can be planned in advance and conducted systematically. For this reason a template for
software testing, a set of steps into which we can place specific test case design techniques and testing methods should be defined for software process.

Testing often accounts for more effort than any other software engineering activity. If it is conducted haphazardly, time is wasted, unnecessary effort is expanded, and even worse, errors sneak through undetected. It would therefore seem reasonable to establish a systematic strategy for testing software

**Type of Testing**

There are two type of testing according their behaviors

- Unconventional Testing
- Conventional Testing

1) **Unconventional Testing**

Unconventional testing is a process of verification which is doing by SQA (Software Quality Assurance) team. It is a prevention technique which is performing from beginning to ending of the project development. In this process SQA team verifies project development activities and insuring that developing project is fulfilling the requirement of the client or not.

In this testing the SQA team follows these methods:

1. Peer review
2. Code walk and throw
3. Inspection
4. Document Verification

2) **Conventional Testing**

Conventional Testing is a process of finding the bugs and validating the project. Testing team involves in this testing process and validating that developed project is according to client requirement or not. This process is a correction technique where testing team find bugs and reporting to the development team for correction on developed project built.

For these testing the testing team using the following methodologies.

**Unit testing**

The primary goal of unit testing is to take the smallest piece of testable software in the application, isolate it from the remainder of the code, and determine whether it behaves exactly as you expect. Each unit is tested separately before integrating them into modules to test the interfaces between modules. Unit testing has proven its value in that a large percentage of defects are identified during its use. In the company as well as seeker registration form, the zero length username and password are given and checked. Also the duplicate username is given and checked. In the job and question entry, the button will send data to the server only if the client side validations are made. The dates are entered in wrong manner and checked. Wrong email-id and web site URL (Universal Resource Locator) is given and checked.

**Integration testing**

Testing is done for each module. After testing all the modules, the modules are integrated and testing of the final system is done with the test data, specially designed to show that the system will operate successfully in all its aspects conditions. Thus the system testing is a confirmation that all is correct and an opportunity to show the user that the system works.

**Validation testing**

The final step involves Validation testing, which determines whether the software function as the user expected. The end-user rather than the system developer conduct this test most software developers as a process called “Alpha and Beta Testing” to uncover that only the end user seems able to find.

The compilation of the entire project is based on the full satisfaction of the end users. In the project, validation testing is made in various forms.

**Testing Strategies**

A number of software testing strategies have been proposed in the literature. All provide the software developer with a template for testing and all have the following generic characteristics:

Testing begins at the component level and works “outward” toward the integration of the entire computer-based system.

1. Different testing techniques are appropriate at different points in time.
2. The developer of the software conducts testing and for large projects, independent test group.
3. Testing and debugging are different activities, but debugging must be accommodated in any testing strategy.

**Testing techniques:**

**Module Testing**

Module Testing is a process of testing the system, module by module. It includes the various inputs given, outputs produced and their correctness. By testing in this method we would be very clear of all the bugs that have occurred.

**Interface Testing**

The Interface Testing is performed to verify the interfaces between sub modules while performing integration of sub modules aiding master module recursively.

**Black Box Testing**

In this testing we give input to the system and test the output. Here we do not go for watching the internal file in the system and what are the changes made on them for the required output.

**White Box Testing**

It is just the vice versa of the Black Box testing. There we do not watch the internal variables during testing. This gives clear idea about what is going on during execution of the system. The point at which the bug occurs were all clear and were removed

**Integration Testing**

The strategies for integrating software components into a functioning product include the bottom-up strategy, the top-down strategy and to ensure that modules will be available for integration into the evolving software product when needed. The integration strategy dictates the order in which modules must be available and thus exerts a strong influence on the order
in which modules are written, debugged and unit tested. 

**Maintenance:**

The objectives of this maintenance work are to make sure that the system gets into work all time without any bug. Provision must be for environmental changes which may affect the computer or software system. This is called the maintenance of the system. Nowadays there is the rapid change in the software world. This is the final step in system life cycle. Here we implement the tested error-free system into real-life environment and make necessary changes, which runs in an online fashion. Here system maintenance is done every months or year based on company policies, and is checked for errors like runtime errors, long run errors and other.

**9. Conclusion**

Packet-dropping attack has always been a major threat to the security in MANETs. In this project, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations.

The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. We have implemented an effective intrusion detection system called “EAACK” (Enhanced Adaptive Acknowledgement) by which we can identify and protect the network from malicious activities. Also by identify the Genuine / attacker’s loss will also increase the security level in mobile ad hoc networks.

**10. Future enhancement**

The data can also be lost due to the Low Buffer level of the node. So we are also calculating the Buffer Level of each node. By calculating the buffer level, we can identify whether it is normal data loss or data loss due compromise of the node. Security level will be increased due to the Encrypting the data packet, also that the acknowledgment from each node will denote that the data packets are send safely. We can also identify that the packet loss can occur due to the low buffer level problem.

**References**


