Trust Based Ad-hoc on Demand Routing Protocol for MANET

Vijaya Krishna Sonthi
Assistant Professor,
Dept of CSE,
Sasi Institute of Technology and Engineering,
Tadepalligudem.

Bala Bhaskara Rao Emani
Assistant Professor,
Dept of CSE,
Sasi Institute of Technology and Engineering,
Tadepalligudem.

Abstract:

Mobile Ad-hoc networks (MANET) is a set of wireless nodes without any fixed infrastructure or base station, in which nodes communicate directly to the other nodes within its transmission range over relatively bandwidth constrained wireless links. MANET is vulnerable to various types of attacks from malicious nodes due to its spontaneous nature of communication and the absence of centralized administrator. There are many attacks in MANET due to which the legitimacy of a network is compromised such as, Black Hole Attack, Worm Hole Attack, Byzantine attack, DoS attack. So, secure communication in MANET is essential and challenging task. In this paper, we present trust based Ad hoc On Demand Routing protocol for MANET. Our proposed algorithm works on the concept of honest value which is calculated on the concept of hop and trust to protect the network from malicious node. The performance of the proposed protocol is analyzed using throughput, number of drop packets, packet delivery ratio and number of received packets with the variation of number of nodes, speed and simulation time. Results show that the proposed method has better performance and enhance the security in the network.

INTRODUCTION:

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other independent of the network architecture.

MANETs have a wide area of applications in battlefield, rescue work, as well as civilian applications like an outdoor meeting, or an Ad-hoc classroom. With the increasing number of applications to harness the advantages of Ad Hoc Networks, more concerns arise for security issues in MANETs. With the wide range of applications of MANET security challenges also have to be dealt. The wireless network with their easy to access as an advantage is bound to have some target areas in it.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Project Implementation:

Module Description:

Mobile Relays:

The network consists of mobile relay nodes along with static base station and data sources. Relay nodes do not transport data; instead, they move to different locations to decrease the transmission costs. We use the mobile relay approach in this work. Goldenberg et al. [13]

showed that an iterative mobility algorithm where each relay node moves to the midpoint of its neighbors converges on the optimal solution for a single routing path. However, they do not account for the cost of moving the relay nodes. In mobile nodes decide to move only when moving is beneficial, but the only position considered is the midpoint of neighbors.

Sink:

The sink is the point of contact for users of the sensor network. Each time the sink receives a question from a user, it first translates the question into multiple queries and then disseminates the queries to the corresponding mobile relay, which process the queries based on their data and return the query results to the sink. The sink unifies the query results from multiple storage nodes into the final answer and sends it back to the user.

Source Nodes:

The source nodes in our problem formulation serve as *storage points* which cache the data gathered by other nodes and periodically transmit to the sink, in response to user queries. Such a network architecture is consistent with the design of storagecentric sensor networks [38]. Our problem formulation also considers the initial positions of nodes and the amount of data that needs to be transmitted from each storage node to the sink.

Tree Optimization:

We consider the subproblem of finding the optimal positions of relay nodes for a routing tree given that the topology is fixed. We assume the topology is a directed tree in which the leaves are sources and the root is the sink. We also assume that separate messages cannot be compressed or merged; that is, if two distinct messages of lengths m1 and m2 use the same link (si, sj) on the path from a source to a sink, the total number of bits that must traverse link (si, sj) is m1 + m2.

INPUT DESIGN:

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

What data should be given as input?

How the data should be arranged or coded?

The dialog to guide the operating personnel in providing input.

Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES:

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN:

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

Convey information about past activities, current status or projections of the

Future.

Signal important events, opportunities, problems, or warnings.

Trigger an action.

Confirm an action.

SYSTEM ANALYSIS

EXISTING SYSTEM

Wireless Multimedia Sensor Networks (WMSNs) has many challenges such as nature of wireless media and multimedia information transmission. Consequently traditional mechanisms for network layers are no longer acceptable or applicable for these networks.

PROPOSED SYSTEM

We use low-cost disposable mobile relays to reduce the total energy consumption of dataintensive WSNs. Different from mobile base station or data mules, mobile relays do not transport data; instead, they move to different locations and then remain stationary to forward data along the paths from the sources to the base station. Thus, the communication delays can be significantly reduced compared with using mobile sinks or data mules. Moreover, each mobile node performs a single relocation unlike other approaches which require repeated relocations.

Literature survey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

Overview

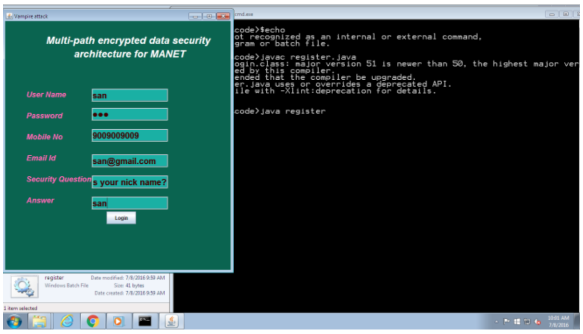
A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on and may improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified.Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad hoc networks to be formed quickly. In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. DoS they say is a tool for registering dissent. Richard Stallman has stated that DoS is a form of 'Internet Street Protests’. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Results



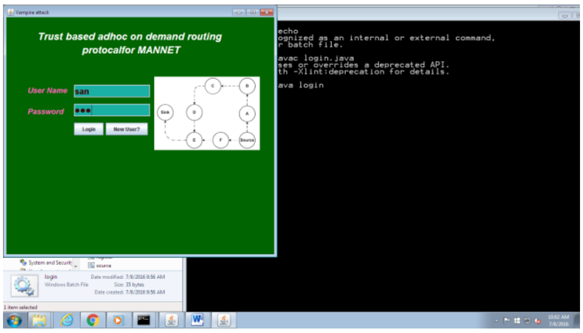
Multi-path encrypted data security architecture for MANET

User Name: san
Password: ●●●
Mobile No: 9009009009
Email Id: san@gmail.com
Security Question: s your nick name?
Answer: san

```
code>$echo
ot recognized as an internal or external command,
gram or batch file.

code>javac register.java
ogin.class: major version 51 is newer than 50, the highest major ver
ed by this compiler.
ended that the compiler be upgraded.
er.java uses or overrides a deprecated API.
ile with -Xlint:deprecation for details.

code>java register
```



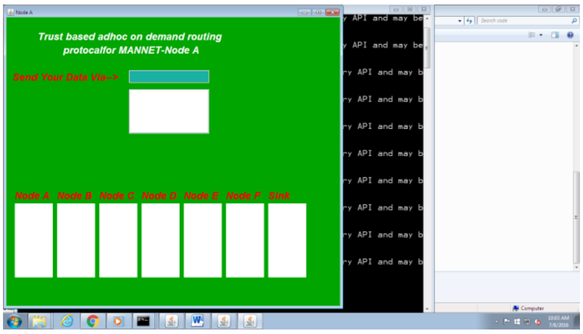
Trust based adhoc on demand routing protocalfor MANNET

User Name: san
Password: ●●●

```
echo
ognized as an internal or external command,
r batch file.

avac login.java
ses or overrides a deprecated API.
th -Xlint:deprecation for details.

ava login
```



Trust based adhoc on demand routing protocalfor MANNET-Node A

Send Your Data Via-->

```
y API and may be
y API and may be
ry API and may b
ry API and may b
ry API and may b
ry API and may b
ry API and may b
ry API and may b
ry API and may b
ry API and may b
```

CONCLUSION:

Mobile Ad-hoc network (MANETs) has many challenges due to its dynamic nature. Some of the major challenges are number of malicious nodes detected, number of hops, route discovery time and packet loss. Routing algorithms namely DMR, TMR and MTMR have their own way in order to establish the trust and transmit packet securely.

But message trust based multipath routing protocol proved to be best in terms of number of malicious nodes detected, number of hops, route discovery time and packet loss.

REFERENCES:

[1]D.Umuhoza, J.I.Agbinya,andC.W.Omlin,“Estim tion of Trust Metrics for MANET using QoS Parameters and Source Routing Algorithms” Second International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney NSW, ISBN: 978-0-7695-2846-5, DOI:

10.1109/AUSWIRELESS.2007.3, IEEE Computer Society 10 September 2007.

[2] Ming Yu, Mengchu Zhou, and Wei Su, “A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments” IEEE Transactions on Vehicular Technology, Volume: 58, Issue: 1, ISSN: 0018-9545, DOI:

10.1109/TVT.2008.923683, pp. 449-460, 13 January 2008.

[3]Xu Yi, Cui Mei, Yang Wei, and Xan Yin, “ A Node-disjoin Multipath Routing in Mobile Ad hoc Networks”, IEEE International Conference on Electric Information and Control Engineering (ICEICE-2011), School of Computer Science and Technology, Wuhan University of Technology Wuhan, China, ISBN: 978-1-4244-8039-5, pp. 1067-1070, DOI: 10.11O9/ICEICE.2011.5777190, IEEE 27th May 2011.

[4] SungHwi Kim, SeungMin oh, HoSung Park, Jeongcheol Lee, and SangHa Kim, “Disjoint Multipath Scheme with Hole Detouring Strategy in Wireless Sensor Networks” IEEE Vehicular Technology Conference (VTC Fall), San Francisco, CA, ISBN: 978-1-4244-8328-0, DOI:

10.11O9/VETECF.2011.6093219, pp. 1-5, 01 December 2011.

[5]Jassim H.S, Yussof S, Tiong Sieh Kiong, Koh S.P, and Ismail R, “A routing protocol based on trusted and shortest path selection for mobile Ad hoc network” IEEE 9th International Conference on Communications (MICC), Kuala Lampur, Malaysia, ISBN:978-1-4244-5531, DOI:

10.11O9/MICC.2009.5431438, pp. 547-554, 15th March 2010.

[6] X. Li Z, Jia P, Zhang R, Zhang H, and Wang, " Trust-based on-demand multipath routing in mobile ad hoc networks" The Institution of Engineering and Technology(IET), School of Computer Science & Technology, Shandong Univ., Ji'nan, China, Volume: 4, Issue: 4, ISSN: 1751-8709, DOI:

10.1049/iet-ifs.2009.0140, pp. 212-232, 20th December 2010.

[7]Lacharite, Y.Dang Quan Nguyen, Maoyu Wang, and Lamont L, "A Trust-based Security architecture for tactical MANETs" IEEE Military Communications Conference, (MILCOM 2008), San Diego, CA, ISBN: 978-1-4244-2676-8, DOI: 10.1109/MILCOM.2008.4753215, pp. 1-7, 19 January 2009.