International Journal of Smart Sensor and Adhoc Network

Volume 2 | Issue 3 Article 6

April 2012

NOVEL DEFENCE MECHANISM AGAINST ON DEMAND ADHOC ROUTING PROTOCOL FOR MOBILE ADHOC NETWORKS

K. SUBBA RAO
Department of IT, St ann's Engineering College, subbukatte@gmail.com

N. PRAGINA
SEfrom St ann's EngineeringCollege., pragna.nallapaneni@gmail.com

NOVEL DEFENCE MECHANISM AGAINST ON DEMAND ADHOC ROUTING PROTOCOL FOR MOBILE ADHOC NETWORKS

K.SUBBA RAO[1] **& N.PRAGINA**[2]

[1]Department of IT, St ann's Engineering College,
[2]Pursuing Master Degree in SEfrom St ann's EngineeringCollege.
Email:subbukatte@gmail.com, pragna.nallapaneni@gmail.com

Abstract:To access multimedia data mobile users like to use their own consumer electronic devices anywhere and at anytime . Hence, we expect that wireless ad hoc networks will be widely used in the near future since these networks form the topology with low cost on the fly. However, consumer electronic devices generally operate on limited battery power and therefore are vulnerable to security threats like data flooding attacks. The data flooding attack causes Denial of Service (DoS) attacks by flooding many data packets. However, there are a few existing defense systems against data flooding attacks. Moreover, the existing schemes may not guarantee the Quality of Service (QoS) of burst traffic since multimedia data are usually burst. Therefore, we propose a novel defense mechanism against data flooding attacks with the aim of enhancing the throughput. The simulation results show that the proposed scheme enhances the throughput of burst traffic.

Keywords *— Data flooding attack, throughput, burst traffic, wireless ad hoc network.*

I. INTRODUCTION:

Consumer electronic devices have evolved depending on user needs. Users want to use compact and portable devices such as cellular phones, laptop computers, Personal Digital Assistants (PDAs), etc. anywhere and at anytime [1]. They like to use those devices to download multimedia data or to access real-time traffic. Those devices are used as mobile nodes in wireless ad hoc networks; hence, wireless ad hoc networks on the basis of consumer electronics are expected to be widely used in the near future. In wireless ad hoc networks, the communications take place between mobile nodes, operating under limited energy of battery power rather than through base stations [2]. Hence, it becomes extremely hazardous to wireless ad hoc networks when mobile nodes are clogged. Meanwhile, wireless ad hoc networks are vulnerable to security threats since all signals go through bandwidth constrained wireless links and the routing decision are taken in a decentralized manner [3].

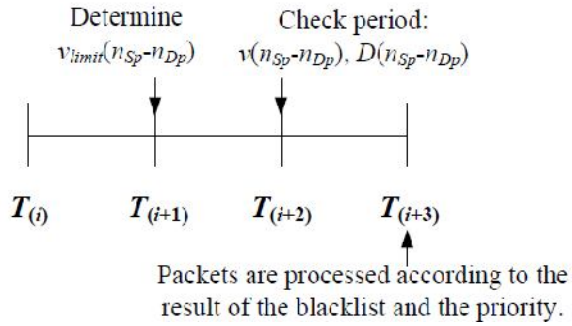
Therefore, it is important to provide a path with secure robustness in wireless ad hoc networks. Wireless ad hoc networks can be victimized to various kinds of attacks [4]-[7]. Among them, the ad hoc flooding attack can easily cause Denial-of-Service (DoS) attacks by flooding many Route Request (RREQ) or data packets [7]. Since a mobile node has limited resource capacities such as memory space, computational ability, battery power, bandwidth capacity, and so on, it cannot provide services when it receives a lot of packets. Hence, the whole network as well as the victim node can get easily paralyzed. Even though attackers are able to conduct ad hoc flooding attacks by flooding either RREQ packets or data packets, most researches in this field have focused their study on RREQ flooding attacks much more than data flooding attacks [8]-[9]. Contrary to other networks, the path construction from the source node to the destination node is important in wireless ad hoc networks because the communication is performed via multiple hops without any infrastructure. Besides, the data flooding attack can be performed only after constructing a path. Therefore, an attacker sets up a path to the victim node so as to conduct data flooding attacks and then forwards tremendous useless data packets to the victim node along the path. However, the size of data packets is usually much larger than that of RREQ packets; i.e., 24 bytes for RREQ packets and 1 Kbytes or 512 bytes for data packets [10]. Hence, resource consumption and bandwidth congestion of a node or the entire network can be easily occurred by data flooding attacks.

The flooding attack prevention (FAP) [7] suggested a defense system against either RREQ or data flooding attacks. The path cut off mechanism is used as defense against data flooding attacks [7]. When the victim node realizes that it has been subjected to the data flooding attack, it may cut off the path. However, the procedure of the path cut off mechanism is not explained in detail, and FAP cuts off the path when many data packets are transmitted to the victim node. Current users like to download or access multimedia data using the consumer electronic devices so that the packets may be transferred as burst traffic [11]. However, FAP cannot distinguish burst traffic from attack traffic since FAP distinguishes an attack by comparing the incoming packets with a threshold. Hence, the throughput of burst traffic may degrade if a simple threshold-based defense system is used in FAP.

II. PERIOD-BASED DEFENSE MECHANISM AGAINST DATA FLOODING ATTACKS

To defend the data flooding attack, the proposed PDM scheme sets up *w* periods for the data transmission. The PDM scheme checks data packet floods at the end of each period in order to enhance the throughput of burst traffic. Therefore, it can guarantee the Quality of Service (QoS) of burst traffic.

We denote $v(n_{Sp}\text{-}n_{Dp})$ as the variance of the number of received data packets for the source node (n_{Sp}) to the destination node (n_{Dp}) during the period $T_{(i+1)}\text{-}T_{(i+2)}$. Here, *p* denotes the number of sessions taken for data transfer.



III. SYSTEM ANALYSIS

Existing system:

Ranging and positioning techniques are highly vulnerable to attacks from dishonest nodes and external attackers; dishonest nodes can report false position and distance information in order to cheat on their locations; external attackers can spoof measured positions of honest nodes. An attacker can generally influence all thesemeasurements by jamming and delaying signals, and by modifying their signal strengths.

Proposed system:

We propose a different approach to secure data's while transferring, that relies on a set of covert base stations used for secure positioning to find the attack particularly. A novel period-based defense mechanism (PDM) against data flooding attacks taking enhancing the throughput of burst traffic into account.

IV. PROBLEM FORMULATION

4.1 Objective:

Mobile users like to use their own consumer electronic devices anywhere and at anytime to access multimedia data. Hence, we expect that wireless ad hoc networks will be widely used in the near future since these networks form the topology with low cost on the fly. However, consumer electronic devices generally operate on limited battery power and therefore are vulnerable to security threats like data flooding attacks. The data flooding attack causes Denial of Service (DoS) attacks by flooding many data packets. However, there are a few existing defense systems against data flooding attacks. Moreover, the existing schemes may not guarantee the Quality of Service (QoS) of burst traffic since multimediadata are usually burst. Therefore, we propose a novel defense mechanism against data flooding attacks with the aim of enhancing the throughput.

4.2 Hardware Specification

- SYSTEM : Pentium IV 2.4 GHz
- HARD DISK : 40 GB
- FLOPPY DRIVE : 1.44 MB
- MONITOR : 15 VGA colour
- MOUSE : Logitech.
- RAM : 256 MB
- KEYBOARD : 110 keys enhanced

4.3 Software Specification

- Operating system :- Windows XP Professional
- Front End :- Java Technology
- Tool : Eclipse

4.4 Software Description

Java Technology

Java technology is both a programming language and a platform.

V. THE JAVAPROGRAMMING LANGUAGE

The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust

- With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called *Java byte codes* —the platform-independent codes interpreted by the interpreter on the Java

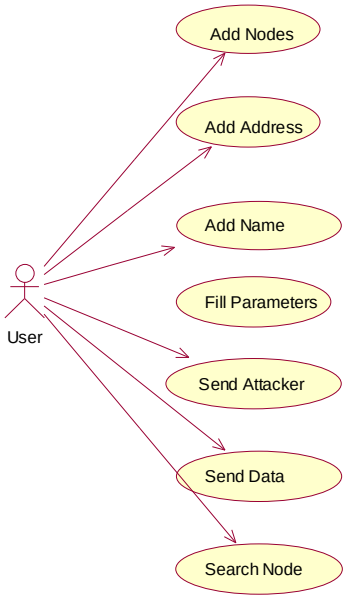
platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilationhappens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works

VI. SYSTEM DESIGN:

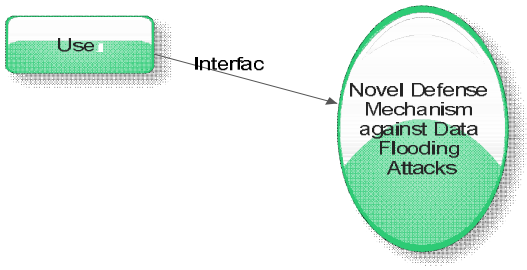
DESIGN OVERVIEW:

Design involves identification of classes, their relationships as well as their collaboration. In objectory, classes were divided into Entity classes, interface classes and the control classes. The Computer Aided Software Engineering tools that are available commercially do not provide any assistance in this transition. Even research CASE tools take advantage of meta modeling are helpful only after the construction of class diagram is completed. In the Fusion method ,it used some object-oriented approaches like Object Modeling.

Use case diagram:

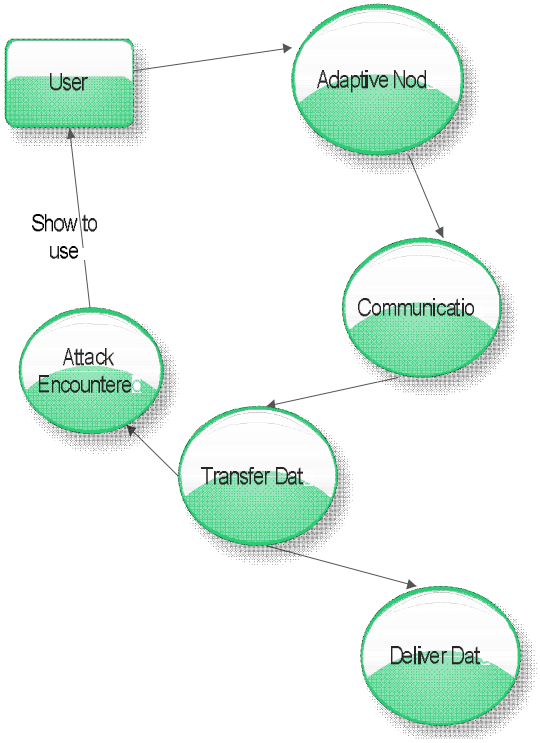


Contextanalysis diagram:

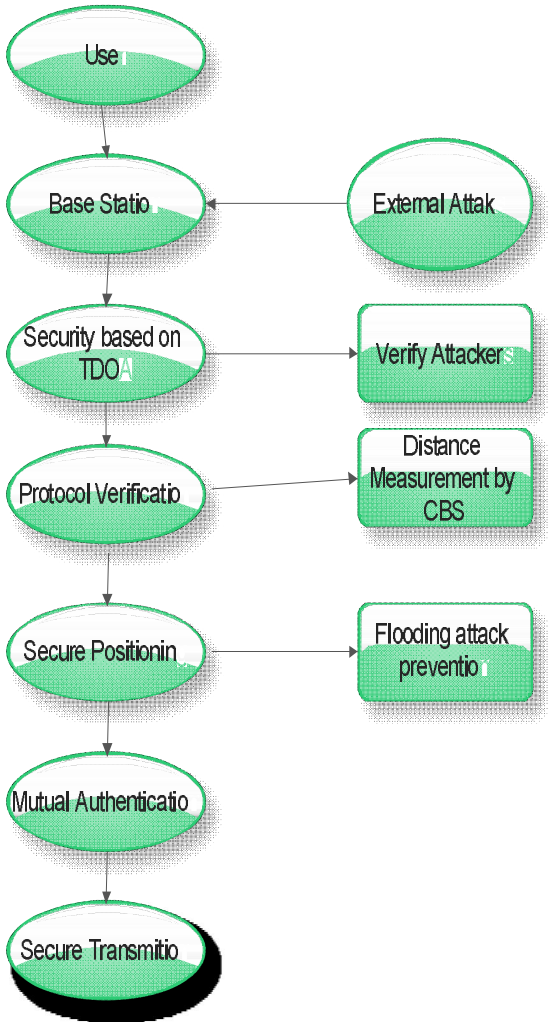


DATA FLOW DIAGRAM:

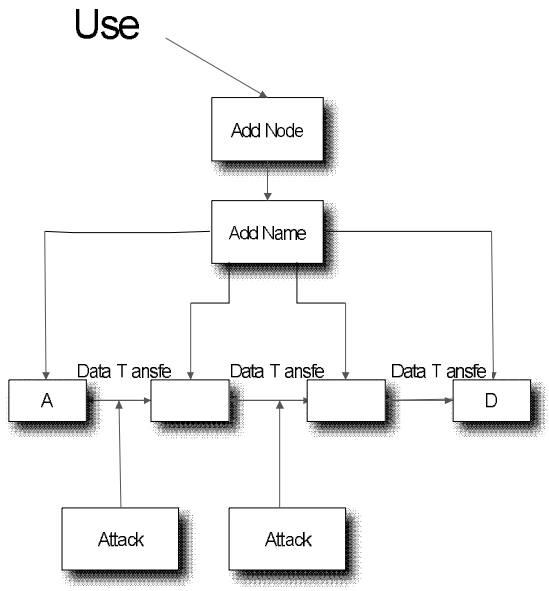
Level1 DFD:



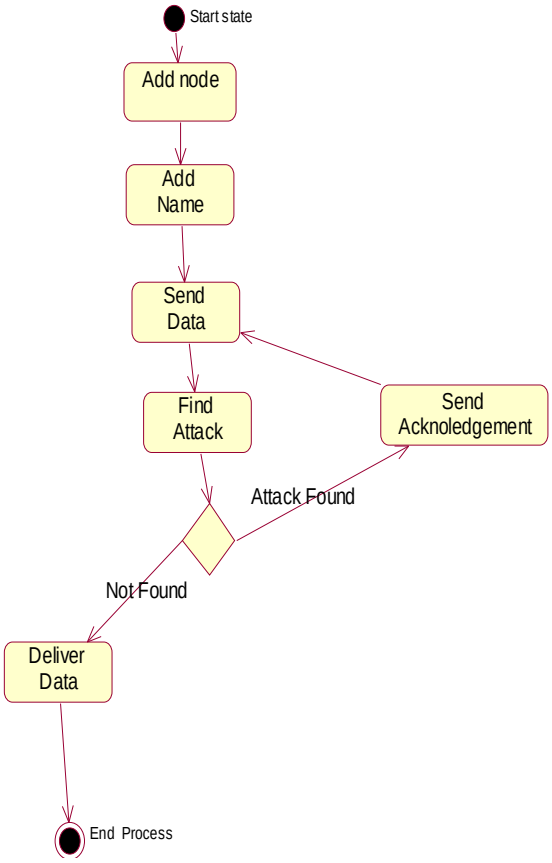
Level2 DFD:



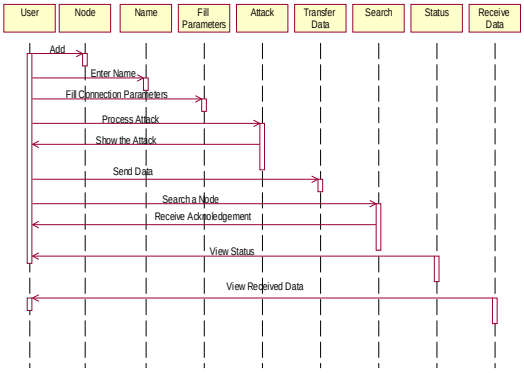
SYSTEM ARCHITECTURE:



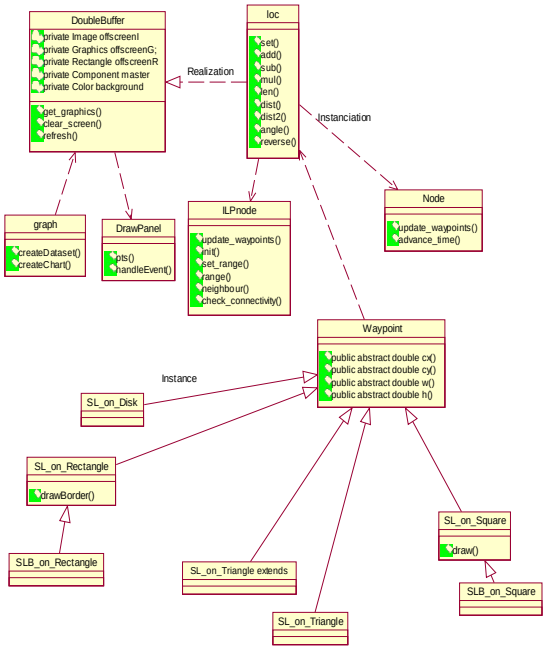
ACTIVITY DIAGRAM:



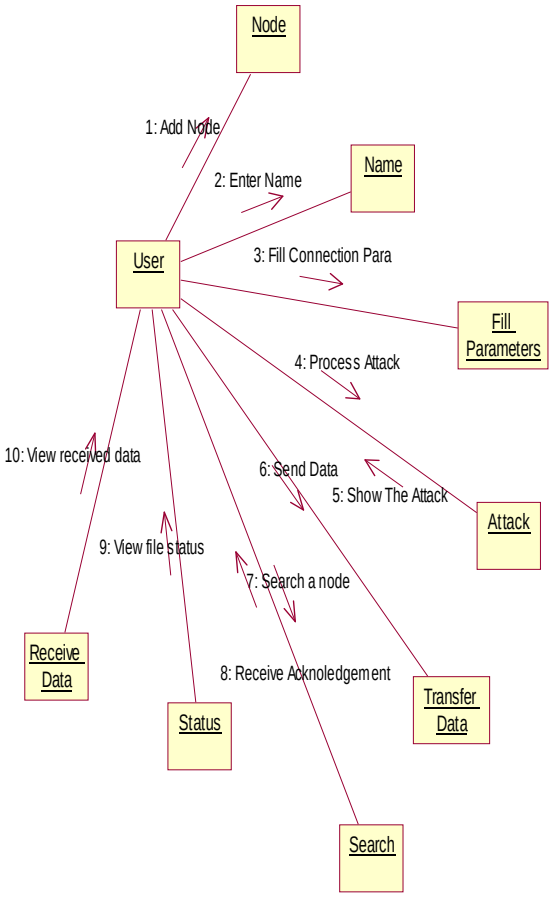
SYSTEM CASE DIAGRAM:



CLASS DIAGRAM:



COLLABRATION DIAGRAM:



CONCLUSION:

We have proposed the period-based defense mechanism against data flooding attacks. The data flooding attack paralyzes a victim node by consuming its resources. Hence, the throughput of the victim node is significantly reduced. However, the current defense systems focus on RREQ flooding attacks rather than the data flooding attack. They easilyattack paralyzes a victim node by consuming its resources.

Hence, the throughput of the victim node is significantly reduced. However, the current defense systems focus on RREQ flooding attacks rather than the data flooding attack. They easily reduce the throughput of burst traffic by comparing with the simple threshold. Hence, we scheme uses a blacklist, considers the data type, and processes packets according to the priority aim to enhance the throughput of burst traffic under the data flooding attack. The proposed so as to defend against data flooding attacks; since the attacker forwards many data packets at a high rate for the whole session. Recently, many users like to download and share multimedia data, so we expect that the proposed scheme is useful to networks where burst traffic are transferrable.

BIBLIOGRAPHY AND REFERENCES

[1] A. Jamalipour, "Self-organizing networks [message from the editor-in-chief],"*IEEE Wireless Communications*, vol. 15, no. 6, pp.2-3, Dec. 2008.

[2] S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths inad hoc networks," *IEEE International Conference on Communications (ICC2001)*, vol. 10, pp. 3201-3205, Jun. 2001.

[3] L. Xia and J. Slay, "Securing wireless ad hoc networks: towards a mobile agentsecurity architecture," *the 2nd Australian Information Security ManagementConference 2004 (InfoSec 2004)*, Nov. 2004.

[4] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," *the 42nd annual Southeast regional conference ACM SoutheastRegional Conference (ACMSE 2004)*, pp. 96-97, Apr. 2004.

[5] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole attacks in wireless networks,"*IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370-380, Feb. 2006.

AUTHOR'S PROFILE:

1. K..Subbarao working as associate professor of IT department in st.ann's college of engineering.
2. N.pragina pursing master degree with software engineering in st.ann's college of engineering.