New-fangled Method against Data Flooding Attacks in MANET

Kavuri Roshan[1], K.Reddi Prasad[2], Niraj Upadhayaya[3] & A.Govardhan[4]
[1, 2&3]Department of Computer Science & Information Technology,
J.B. Institute of Engineering & Technology, Hyderabad, Andhra Pradesh INDIA,
[4]Department of Computer Science. JNTUH,Kukatpally,Hyderabad, INDIA

[1]**Phone No: 09949106818, Email :** [1]*roshan.kavuri@gmail.com*
[2]*reddiprasad.jbit@gmail.com,,* [3]*nirajup@ieee.org,*
[4]*govardan_cse@yahoo.co.in*

ABSTRACT

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 defence 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 defence mechanism against data flooding attacks with the aim of enhancing the throughput.

KEYWORDS

*Data **F**looding attack, Throughput, Bursttraffic, Wireless ad hoc Network.*

1. 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

DOI : 10.5121/ijcsit.2012.4303

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.

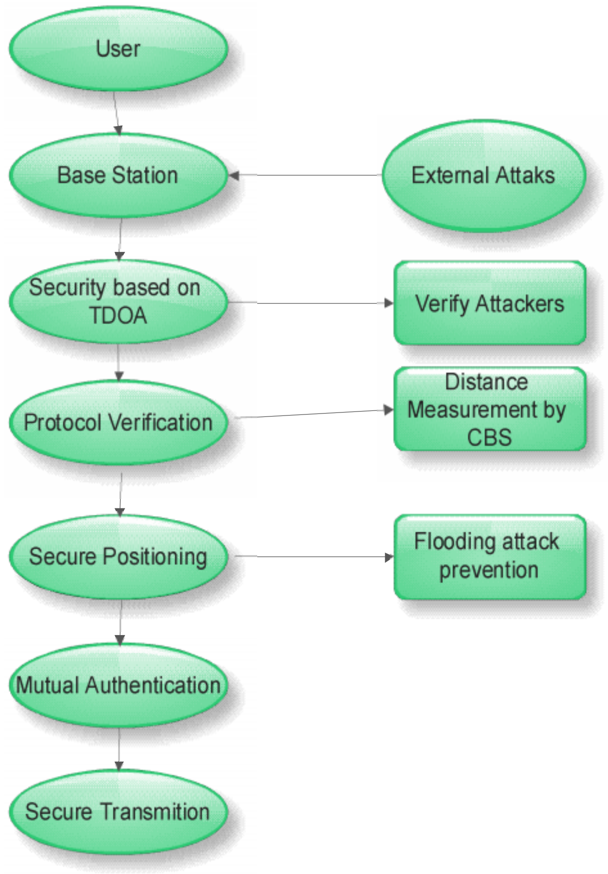
The flooding attack prevention (FAP) [7] suggested a defence system against either RREQ or data flooding attacks. The path cut off mechanism is used as defence against data flooding attacks [7]. When the victim node realizes that it has been subjected to the data flooding attack, it may cut off the path. 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 defence system is used in FAP.

Therefore, this paper proposes a novel period-based defence mechanism (PDM) against data flooding attacks taking enhancing the throughput of burst traffic into account. The proposed PDM scheme is based on periods and uses a blacklist to efficiently prevent the data flooding attack, as a result of which many data packets are forwarded at a high rate for the whole duration. The rest of the paper is organized as follows: Section 2 measures the throughput of burst traffic under data flooding attacks, and then Section 3 presents the proposed PDM scheme. Section 4 shows the performance evaluation of the PDM scheme. Finally, Section 5 concludes the paper.

2. PRELIMINARIES

2.1. Data Flow Diagrams:

A DFD shows what kinds of data will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.



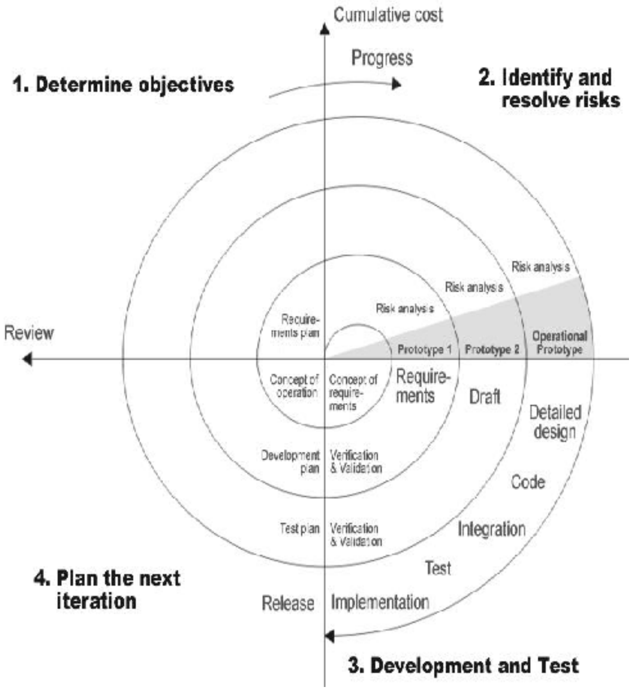
2.2. Title

2.2. SDLC Methodologies:

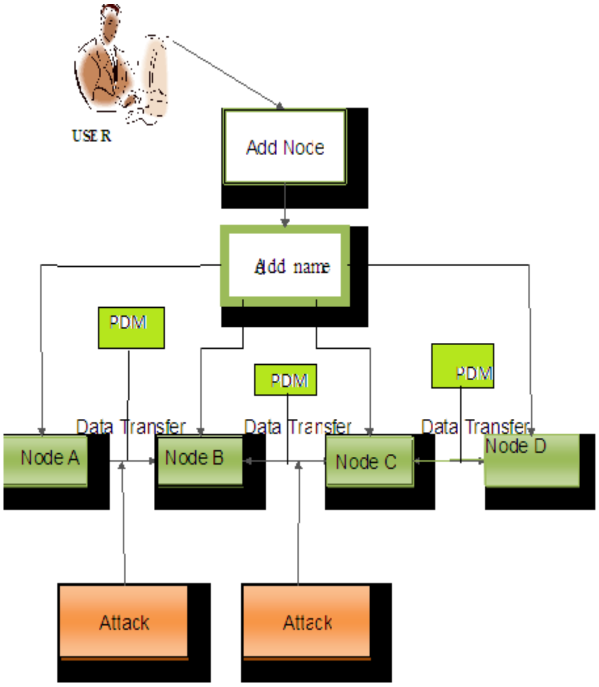
This document play a vital role in the development of life cycle (SDLC) as it describes the complete requirement of the system. It means for use by developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process.

Spiral model was defined by Barry Boehm in his 1988 article, “A spiral Model of Software Development and Enhancement. This model was not the first model to discuss iterative development, but it was the first model to explain why the iteration models.

As originally envisioned, the iterations were typically 6 months to 2 years long. Each phase starts with a design goal and ends with a client reviewing the progress thus far. Analysis and engineering efforts are applied at each phase of the project, with an eye toward the end goal of the project.



3. SYSTEM ARCHITECTURE AND IMPLIMENTATION



3.1. MODULES

Throughput of Burst Traffic under Data Flooding Attacks.
Period –Based Defence Mechanism against Data Flooding Attacks
Performance Evaluations

Module Description:

3.1.1. Throughput of burst Traffic under Data Flooding attacks

In wireless ad hoc networks, handheld-based consumer electronic devices are used as mobile nodes. The data flooding attack sends many data packets in order to clog not only a victim node but also the entire network since all packets are transmitted via multiple hops. Hence, data flooding attacks are extremely hazardous to wireless ad hoc networks.

To conduct the data flooding attack, an attacker first sets up a path to the victim node since the attack can be performed only after a path is constructed. Then, the attacker forwards tremendous useless data packets along the path to make sure that the victim node cannot process packets in a normal fashion. Finally, the resources of the victim node are exhausted, so the node may get isolated from the network.

In order to measure the effect of the data flooding attack on data traffic including burst traffic in wireless ad hoc networks, we calculate the throughput.

The throughput is defined as the ratio between the amount of data packets sent by the source node and the amount of data packets received by the destination node during a time span from t_s to t_d [12]. The amount of packets sent by the source node (*tr*) can be classified into control packets (*C*) such as RREQ, Route Reply (RREP), Route Error (RERR) packets and data packets (D_{all}) including traffic for conducting data flooding attacks. On the other hand, the amount of data packets received by the destination node (*rc*) can be classified into normal traffic (D_N) excluding the traffic meant for data flooding attacks $(\ \gamma\ )$. Therefore, we can represent the throughput using the following equation:

$$Throughput = \int_{t_s}^{t_d} (\frac{rc}{tr})dt = \int_{t_s}^{t_d} (\frac{D_N - \gamma}{C + D_{all}})dt . \qquad (1)$$

Meanwhile, we can divide the normal traffic into non-burst traffic (α) and burst traffic (β), so D_N is presented as:

$$D_N = \alpha + \beta . \qquad (2)$$

Using (1) and (2), the throughput can be represented as follows:

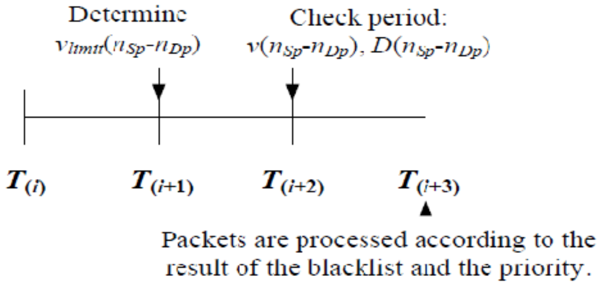
$$Throughput = \int_{t_s}^{t_d} (\frac{\alpha + \beta - \gamma}{C + D_{all}})dt . \qquad (3)$$

Therefore, the throughput is affected when many control packets are huge traffic are deliberately generated so as to conduct data flooding attacks

3.1.2. Period based Defence 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.


Determine
$v_{limit}(n_{Sp}\text{-}n_{Dp})$
Check period:
$v(n_{Sp}\text{-}n_{Dp})$, $D(n_{Sp}\text{-}n_{Dp})$
$T_{(i)}$
$T_{(i+1)}$
$T_{(i+2)}$
$T_{(i+3)}$
Packets are processed according to the result of the blacklist and the priority.

3.1.3. Procedures of each period in the PDM scheme.

This Fig. shows procedures of each period in the PDM scheme. The mobile node n_u initiates the variance coordinator $(h(n_{Sp}\text{-}\ \ n_{Dp}))$ for data packet floods from n_{Sp} to n_{Dp}according to its data type so as to guarantee the QoS of the data packets. We also assume that *ave*(*all*) is the average number of all received data packets during $T_{(i)}\text{-}T_{(i+1)}.$Then, we determine the variance limit of data packet floods from n_{Sp} to n_{Dp} $(v_{limit}(n_{Sp}\text{-}n_{Dp}))$ using the following equation:

$$v_{limit}(n_{Sp}-n_{Dp})=ave(all)+h(n_{Sp}-n_{Dp}). \qquad (4)$$

3.1.4. The procedure of the PDM scheme is following as:

Step 1) At the end of the period $T_{(i+2)}$, n_u compares the variance of received data packets, according to the $n_{Sp}\text{-}n_{Dp}$ pair $(v(n_{Sp}\text{-}n_{Dp}))$, with the variance limit $(v_{limit}(n_{Sp}\text{-}n_{Dp}))$. In wireless ad hoc networks, all packets are transferred via links between mobile nodes so that we can defend against data flooding attacks through the entire network by performing the defence at each mobile node.

Step 2) When $v(n_{Sp}\text{-}n_{Dp})$ is greater than $v_{limit}(n_{Sp}\text{-}n_{Dp})$, it checks whether data packets for $n_{Sp}\text{-}n_{Dp}$ pairs $(D(n_{Sp}\text{-}n_{Dp}))$are in the blacklist or not. The blacklist is maintained by each mobile node, which is initially empty. The maximum number of received data packets for a certain source node – destination node pair is listed in the blacklist. It aims to detect data flooding attacks.

Step 2-1) If $D(n_{Sp}\text{-}n_{Dp})$ is in the blacklist, it is not transmitted until the next period $(T_{(i+3)})$.

Step 2-2) Else, priority is determined by the inversion of the number of received data packets and n_u processes the data packets according to priority.

Step 3) n_u updates the blacklist by the greatest number of received data packets in the period.

Step 4) n_u checks the period is the last period of the data transmission.

Step 4-1) If it is the last period, the procedure of the PDM scheme is stopped.

Step 4-2) Else, go to Step 1.

4. PERFORMANCE EVALUATION.

4.1. Throughput Comparison

The performance of the proposed PDM scheme is measured by the throughput as given in (1). The PDM scheme sets up *w* periods for the data session from t_s to t_d to defend the data flooding attack. The PDM scheme guarantees the QoS of non-burst traffic as well as burst traffic by determining $v_{limit}(n_{Sp} - n_{Dp})$ depending on the data type. The PDM scheme utilizes the blacklist since the data packet flooding attacker sends a high rate of data packets all times rather than certain given durations. Moreover, the PDM scheme collects the information for calculating $v_{limit}(n_{Sp} - n_{Dp})$ at the first period and then performs the defence mechanism. Therefore, the expected probability of the received malicious data traffic in the PDM scheme at n_u ($E_{PDM}[\gamma]$) is as:

$$E_{PDM}[\gamma] = \sum_{v=2}^{n}\{ \int_{t=T_v}^{T_{v+1}} (E[\gamma])dt\}. \qquad (5)$$

The PDM scheme can defend against malicious traffic which are burst and listed in the blacklist. Moreover, it processes the rest of data packets according to priority so that it can defend some of other malicious traffic. Hence, we can rewrite (5) as (6).

$$E_{PDM}[\gamma] \approx \sum_{v=2}^{n}\{ \int_{t=T_v}^{T_{v+1}} (E[U \times L])dt\}. \qquad (6)$$

Here, we denote $U \times L$ as the burst malicious traffic which are also listed in the blacklist. Hence, the malicious traffic (γ') that the victim node receives can be presented as follows: $\gamma' = U \times L$. (7) The PDM scheme can prevent bandwidth congestion caused by the data flooding attack, so the amount of control packets of the PDM scheme (C') is reduced much more than C (the amount of control packets when the defence system against the data flooding attack is not operated).

Hence, C' << C. Moreover, the PDM scheme can reduce the total generated number of data packets so that $D'_{all} << D_{all}$ where D'_{all} is D_{all} of the PDM scheme. By reducing the received traffic for conducting the data flooding attack at the victim node, the received normal traffic regardless of burst traffic are increased. Hence, the victim node receives much larger number of received non-burst traffic (α') and burst traffic (β')than the case when the PDM scheme is not conducted.

Therefore, according to (3), the throughput of the PDM scheme $(Throughput_{PDM})$ under the data flooding attack can be presented as the following equation:

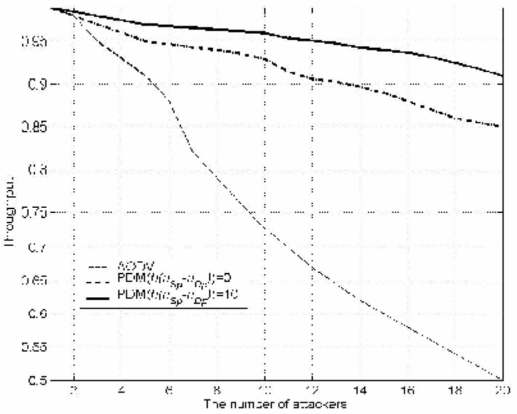
$$Throughput_{PDM} \approx \sum_{v=2}^{n}\{\int_{t=T_v}^{T_{v+1}}(\frac{\alpha'+\beta'-\gamma'}{C'+D'_{all}})dt\}. \qquad (8)$$

Since malicious data packet floods are usually generated at a high rate all the time, β' is extremely improved but γ' is decreased as in (3). Therefore, the throughput of the PDM scheme is improved.

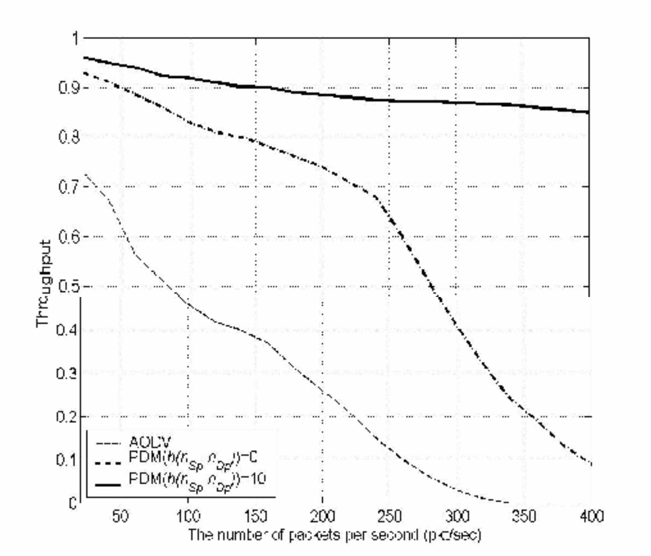
4.2. Simulations

We evaluate the throughput of the PDM scheme using the ns-2 simulation [13]. We conduct the simulation for 100 times and then draw the mean value on the graphs. We use 50 mobile nodes which move based on the random waypoint model with the speed of 20 m/s in a 1000 m by 1000 m area for 500 seconds. The transmission range of each node is 250 m. There are 20 CBR sources which send 512-byte UDP packets.

We use the AODV as the basis routing protocol and compare its performance with that of our PDM scheme. We define $h(n_{Sp}\text{-}n_{Dp})$ as 0 and 10 to investigate how the PDM scheme can guarantee QoS of burst traffic and non-burst traffic, respectively.



Above fig shows the throughput varying wit the number of attackers from 0 to 20 attackers. To compare the affect of the number of attackers to the throughput, each node including attackers sends 20 packets per second. The throughput of the PDM scheme regardless of $h(n_{Sp}\text{-}n_{Dp})$ is higher than AODV so that it can defend against malicious data packet flooding attacks.



Above fig shows that PDM with $h(n_{Sp}\text{-}n_{Dp})=10$ can guarantee QoS of burst traffic better than others. To investigate how much QoS of burst traffic are guaranteed, we increase the number of data packets per second from 20 packets/sec to 400 packets/sec. We assume that there are 5 attackers. When the number of packets per second is high (burst traffic), AODV cannot process packets because of the resource exhaustion.

5. CONCLUSION

We have proposed the period-based defence 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 defence 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 aim to enhance the throughput of burst traffic under the data flooding attack. The proposed scheme uses a blacklist, considers the data type, and processes packets according to the priority 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 transferred.

REFERENCES

[1] Lee, S.hyun. & Kim Mi Na, (2008) “This is my paper”, ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.

[2] Gizem, Aksahya & Ayes, Ozcan (2009) Communications & Networks, Network Books, ABC Publishers.

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

[4] S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc works," IEEE International Conference on Communications (ICC 2001), vol. 10, pp. 3201-3205, Jun. 2001.

[5] L. Xia and J. Slay, "Securing wireless ad hoc networks: towards a mobile agent security architecture," the 2nd Australian Information Security Management Conference 2004 (InfoSec 2004), Nov. 2004.

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

[7] 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.

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," the 2nd ACM Workshop on Wireless Security, pp. 30-40, Sept. 2003.

[9] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting flooding attacks in ad hoc networks," International Conference on Information Technology: Coding and Computing 2005 (ITCC 2005), vol. 2, pp. 657-662, Apr. 2005.

[10] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," IEEE Wireless Communications and Networking Conference 2005 (WCNC 2005), vol. 4, pp. 2112-536, Mar. 2005.

[11] S. Li, Q. Liu, H. Chen, and M. Tan, "A new method to resist flooding attacks in ad hoc networks," IEEE Wireless Communications, Networking and Mobile Computing 2006 (WiCOM 2006), pp. 1-4, Sep. 2006.

[12] A. Khan, T. Suzuki, M. Kobayashi, W. Takita, and K. Yamazaki, "Packet size based routing for stable data delivery in mobile ad-hoc networks," IEICE Transactions on Communications, vol. E91-B, no. 7, pp. 2244-2254, July 2008.

[13] X. Yang, Y. Shi, M. Zeng, and R. Zhao, "A novel method of network burst traffic real-time prediction based on decomposition," International Conference on Networking (ICN), Lecture Notes in Computer Science, vol. 3420, pp. 784-793, Apr. 2005.

[14] H. Kim, S. Han, and J. Song, "Maximum lifetime paths for the high packet delivery ratio using fast recover in a mobile ad hoc network," International Conference on Computational Science (ICCS 2006), Lecture Notes in Computer Science, vol. 3992, pp.1101-1104, May. 2006.

Author

Mr Roshan Kavuri has obtained his B.E Degrree from Andhra University during 1988-92, and M.Tech (CSE) from JNT University, Kukatpally Hyderabad in January 2004 He is having nearly 20 years of experience in industry as well as faculty of Computer Science and Information Technology Departments. Presently he is pursuing his PhD from JNTUH Hyderabad, his areas of research includes Computer Architecture, Parallel Computing, Operating Systems and Computer networks. Presently he is working as an Associate Professor in J.B.Institute of Engineering &Technology from 2004 on wards