A Mechanism To avoid Data Flooding Attacks in Adhoc Networks

A.JITENDRA[1] & T.SAHITHI[2]
[1]Department of CSE, VR Siddhartha Engineering College,
[2]M.Tech Student,Dept of CSE VR Siddhartha Engineering College.
Email:jittu28@gmail.com, sahithi.thotakura@gmail.com

Abstract: **There is a wide usage of mobiles anywhere and anytime to access the multimedia data. Thus there will be more opportunity for wireless adhoc networks. Because, comparing with the wired networks, wireless networks provide low cost and easy accessibility. But the main disadvantage for Consumer electronic devices were generally operate on limited battery power and therefore are vulnerable to security threats like Data Flooding Attacks. These attacks lead to Denial of Service (DoS) by flooding many data packets. There were some of the defence systems to data flooding attacks. But these systems may not give guarantee to the Quality of Service. Because because of Wireless data transmission the data may be usually burst. Therefore, wepropose a novel defence 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 adhoc Network.***

I. INTRODUCTION

In the present world, use of electronic devices became most essential. Users want to use the compact and portatable devices such as cellular phones, laptop computers, Personal Digital Assistants (PDAs), etc. anywhere and at anytime. 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. 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. Therefore, it is important to provide a path with secure robustness in wireless ad hoc networks. Wireless adhoc networks can be victimized to various kinds of attacks .Among them, the ad hoc flooding attack can easily cause Denial-of-Service (DoS) attacks by flooding many Route Request (RREQ) or data packets . 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.

I. EXISTING SYSTEM

There were Some of the Existing Systems that were able to solve the Denial-of-Service(Dos) attacks by flooding many Route Requests or Data packets. 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. Contrary to other networks, the path construction from the source node to the destination node is important in wireless adhoc 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. Hence, resource consumption and bandwidth congestion of a node or the entire network can be easily occurred by data flooding attacks.

II. PROPOSED SYSTEM

The Proposed System mainly aims for the Security and Data Flooding attacks prevention and finding the problem where the flooding is attacked by using a mechanism. The flooding attack prevention (FAP) suggested a defense system against either RREQ or data flooding attacks. The path cut off mechanism is used as defense against data flooding attacks. 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. 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.

Therefore, this paper proposes a novel period-based defense 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 IV measures the throughput of burst traffic under data flooding attacks, and then Section V presents the proposed PDM scheme. Section VI shows the performance evaluation of the PDM scheme. Finally, Section VII concludes the paper.

III. 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 ts to td. 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 (Dall) 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 (DN) excluding the traffic meant for data flooding attacks (γ). Therefore, we can represent the throughput using the following equation:

$$Throughput \int_{t_s}^{t_d} (\frac{rc}{tr})dt \int_{t_s}^{t_d} (\frac{D_N \square}{C + D_{all}})dt . \quad (1)$$

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

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

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

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

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

IV. PERIOD BASED DEFENCE MECHANISM AGANIST 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*(*nSp*-*nDp*) as the variance of the number of received data packets for the source node (*nSp*) to the destination node (*nDp*) during the period *T*(*i*+1)-*T*(*i*+2). Here, *p* denotes the number of sessions taken for data transfer.

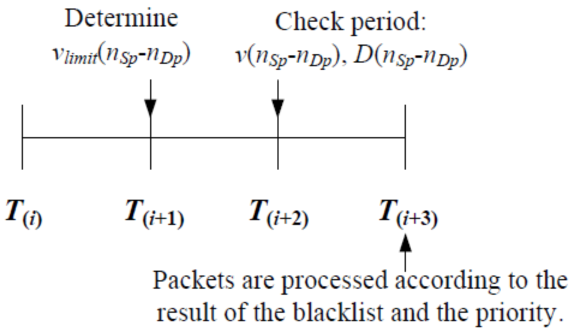

Fig: Procedures of each Period in the PDM Scheme

This shows procedures of each period in the PDM scheme. The mobile node *nu* initiates the variance coordinator (*h*(*nSpnDp*)) for data packet floods from *nSp* to *nDp* 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*)-*T*(*i*+1). Then, we determine the variance limit of data packet floods from *nSp* to *nDp* (*vlimit*(*nSp*-*nDp*)) using the following equation:

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

The procedure of the PDM scheme is following as:

Step 1) At the end of the period *T*(*i*+2), *nu* compares the variance of received data packets, according to the *nSp*-*nDp* pair (*v*(*nSp*-*nDp*)), with the variance limit (*vlimit*(*nSp*-*nDp*)). 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 defense at each mobile node.
Step 2) When *v*(*nSp*-*nDp*) is greater than *vlimit*(*nSp*-*nDp*), it checks whether data packets for *nSp*-*nDp* pairs (*D*(*nSp*-*nDp*)) 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.

i) If *D*(*nSp*-*nDp*) is in the blacklist, it is nottransmitted until the next period (*T*(*i*+3)).
ii) Else, the priority is determined by the inversion of the number of receieved packets and *nu* processes the data packets according to priority.

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

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

i) If it is the last period, the procedure of the PDM scheme is stopped.

ii) Else Goto Step1.

VI. Performance Evaluations

We investigate the performance of the proposed PDM scheme by measuring the throughput. Then, we simulate the throughput of the PDM scheme according to the number of attackers and the number of transferred packets per second by ns-2 simulations.

A. 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 *ts* to *td* to defend the data flooding attack. The PDM scheme guarantees the QoS of non-burst traffic as well as burst traffic by determining **( )** *limit Sp Dp v n* − *n* 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 **( )** *limit Sp Dp v n* − *n* at the first period and then performs the defense mechanism. Therefore, the expected probability of the received malicious data traffic in the PDM scheme at *nu* (**[γ]** *PDM E*) 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:

$$\gamma' = U \times L . \qquad (7)$$

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 defense 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 *all all* $D' << D$ where *all* D' is *all* D 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 (*ThroughputPDM*) 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 $\gamma'$is decreased as in (3). Therefore, the throughput of the PDM scheme is improved.

B. 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*(*nSp-nDp*) as 0 and 10 to investigate how the PDM scheme can guarantee QoS of burst traffic and non-burst traffic, respectively.

Fig. 2 shows the throughput varying with 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*(*nSp-nDp*) is higher than AODV so that it can defend against malicious data packet flooding attacks.

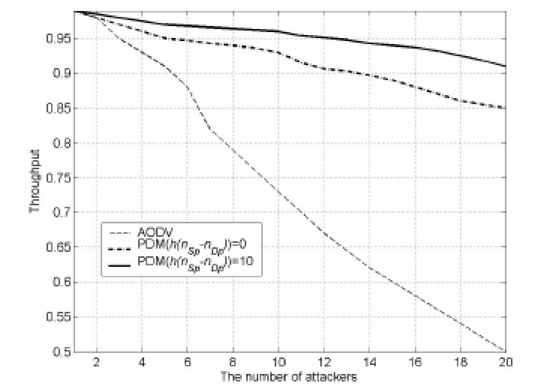

Fig. 2 Throughput vs. the number of attackers.

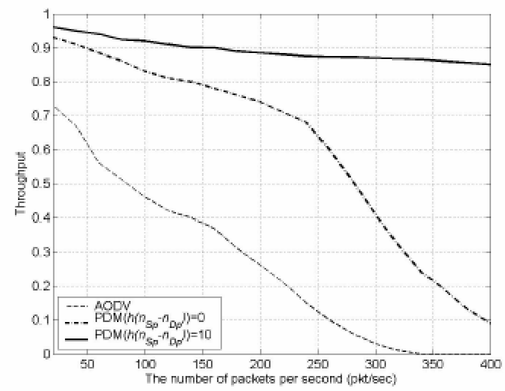

Fig. 3 Throughput vs. the number of packets per second.

Fig. 3 shows that PDM with *h*(*nSp*-*nDp*)=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.

VII. 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 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.

VIII. REFERENCES

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

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

[3] 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.

[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 Southeast Regional 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

