International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Prevention of Data Flooding Attacks using Novel Defense Mechanism in Wireless Ad Hoc Networks

S. N. Uke, A. R. Phirke, D. S. Mahale, S. A . Doshi
Dept. of Information Technology, SKNCOE, Vadgaon (Bk.),
Pune-41, Maharashtra, India

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 few existing defense systems against data flooding attacks. 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.

Keywords

Data flooding attack, throughput, burst traffic

1. INTRODUCTION

Users want to use compact and portable 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. 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 ad hoc networks can be victimized to various kinds of attacks. Attackers are able to conduct ad hoc flooding attacks by flooding either route request packets or data packets.

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 route request packets. Hence resource consumption and bandwidth congestion of a node or the entire network can be easily occurred by data flooding attacks. Thus we suggest flooding attack prevention (FAP) defense system against either route request 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. FAP cuts off the path when many data packets are transmitted to the victim node.

1.1 Problem Statement

In this system, we are going to propose a defense mechanism against data flooding attack

1. To secure data while transferring.
2. To secure positioning of electronic device connected to network.
3. Introducing period based defense mechanism against data flooding attack to enhance the throughput of the system.
4. Evaluating performance of system.

1.2 Need

The number of mobile users is so large and they access multimedia data. They transmit data with the help of wireless communication. These electronic devices have limited power and thus can be easily made victim of security threats like data flooding attacks since all signals go through bandwidth constrained wireless links and the routing decision are taken in a decentralized manner. These data flooding attacks causes Denial of Service (DoS) attack by flooding many data packets. This attack paralyses victim node by consuming its resources. As a result of which throughput of victim node reduces. Therefore we propose a defense mechanism against data flooding attacks to enhance the throughput of the electronic device and also to secure positioning.

2. LITERATURE SURVEY

2.1 Key Terms

Wireless Ad hoc network :-

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 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.

Data Flooding Attack :-
Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host's memory buffer. Once this buffer is full no further connections can be ma, and the result is a Denial of Service.

Burst Traffic :-
A burst is a continuous transfer of data without interruption from one device to another. Burst traffic means any relatively high-bandwidth transmission over a short period, Transmission that combines a very high data signaling rate with very short transmission times. It enables communications between data destination node
and data network operating at dissimilar data signaling rates.

Throughput :-
In communication networks, throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps) and sometimes in data packets per second or data packets per time slot. The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network. The throughput can be analyzed mathematically by means of queuing theory, where the load in packets per time unit is denoted arrival rate , and the throughput in packets per time unit is denoted departure rate.

2.2 Related work done
Resisting Flooding Attacks in Ad Hoc Networks -
Mobile ad hoc networks will often be deployed in environments where the nodes of the networks are unattended and have little or no physical protection against tampering. The nodes of mobile ad hoc networks are thus susceptible to compromise. The networks are particularly vulnerable to denial of service (DOS) attacks launched through compromised node. The intruder broadcasts mass Route Request packets or sends a lot of attacking DATA packets to exhaust the communication bandwidth and node resource so that the valid communication cannot be done. Prevention attack is composed of neighbor suppression and path cutoff. When the intruder broadcasts exceeding packets of Route Request, the immediate neighbors of the intruder observe a high rate of Route Request and then they lower the corresponding priority according to the rate of incoming queries. Moreover, not serviced low priority queries are eventually discarded.

Control Packets Floods in Ad Hoc Networks -
The impact of hacker attacks by malicious nodes affects on overall network performance. Basic route discovery mechanism used in many ad hoc network protocols can be exploited by as few as one malicious or compromised node to bring down the throughput dramatically. An adaptive statistical packet dropping mechanism is used to mitigate such situations and reduce the loss of throughput. The proposed mechanism
works even when the identity of the malicious nodes is unknown and does not use any additional network bandwidth but the network is congested with excess traffic.

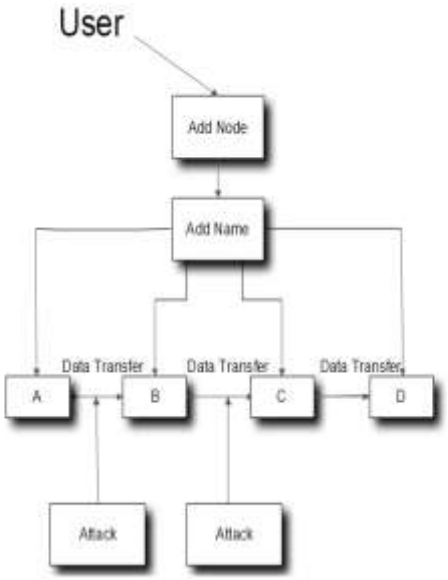
2.3 Existing Methodologies
Ranging and positioning techniques are highly exposed to attack from dishonest nodes and external attackers.
Dishonest nodes can report false position and distance information in order to cheat on their locations.
External attackers can spoof measured positions of honest nodes. An attacker can generally influence all these measurements by jamming and delaying signals and by modifying their signal strengths.

2.3.1 Ranging Technique :-
The end-to-end process of location sensing consists of two sequential phases: (i) measurement (ii) positioning.
For an active cooperative location system where the target S probes the components of the system infrastructure with a physical signal. The measurement phase consists of processing the received signal to estimate parameters of interest such as distance, angle or phase of arrival. The measurements are subsequently
utilized in the positioning phase to compute the location coordinates. The measurement phase is invariably referred to as the ranging phase. Range estimation is a crucial prerequisite for reliable and high accuracy location information as a minor measurement bias will result in positioning errors that scale with increasing distance. The ranging performance depends on: (i) deployment and configuration of the location systems (ii) quality of the ranging waveform and measurement technique. Hence an important research focus on fine-grained localization has been on robust distance estimation.

2.3.2 Positioning Technique :-
Position information of sensors is required by variety of applications such as environmental monitoring and target tracking which directly depend on physical location of node. Due to the demand-initiated self organizing structure of sensor networks sensors are not aware of their locations. Constraints on size, cost and power consumption of nodes make the position estimation in sensor networks challenging. Current state of the art positioning techniques typically use distance measurements from a special set of reference nodes called beacons to estimate their position. A sensor node requires distances from three or more beacons to compute its coordinate. These computations apply multi

alterations techniques to estimate the unknown position. The sensors nodes use signal features for instance Received Signal strength measurements for calculating the distance from the beacons. The attackers can modify the position information of beacons either by spoofing or by compromising the beacon without limit.

3. SYSTEM ARCHITECTURE



4. FUNTIONALITIES

4.1 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 . 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 (γ). Therefore, we can represent the
throughput using the following equation:

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

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

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

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

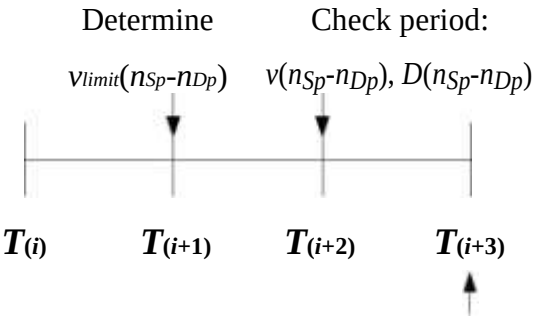
$$Throughput = \int_{t_s}^{t_d} \left(\frac{\alpha + \beta - \gamma}{C + D_{all}}\right) dt . \quad (3)$$

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

4.2 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.



Packets are processed according to the result of the blacklist and the priority.

Fig. 1. Procedures of each period in the PDM scheme.

Fig. 1 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 $T_{(i)}$-$T_{(i+1)}$. 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:

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

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}-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 mobilenodes so that we can defend against data flooding attacks through the entire network by performing the defense at each mobile node.

Step 2) When $v(n_{Sp}\text{-}n_{Dp})$ is greater than $v_{limit}(n_{Sp}\text{-}n_{Dp})$, it checks whether data packets for n_{Sp}-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.

4.3 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* ($[\gamma]\ PDM\ E$) is as:

$$E_{PDM}[\gamma] = \sum\{\int(E[\gamma])dt\} \quad (5)$$

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).

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

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:

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

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 $D'_{all} << D_{all}$ 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:

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

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.

B. Simulations

We evaluate the throughput of the PDM scheme using the ns-2 simulation. 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.

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 $h(n_{Sp}\text{-}n_{Dp})$ is higher than AODV so that it can defend against malicious data packet flooding attacks.

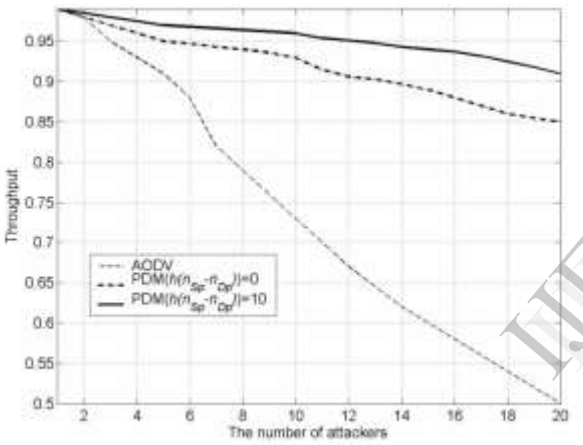


Fig. 2 Throughput vs. the number of attackers.

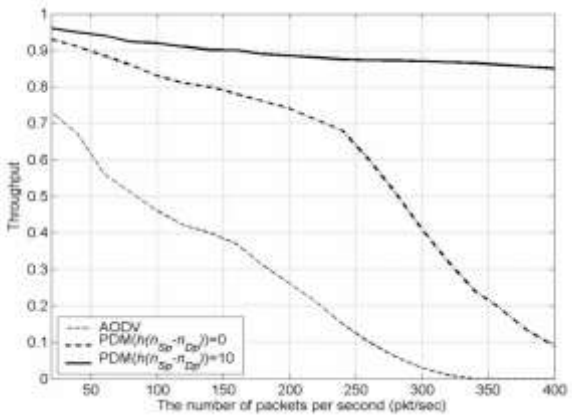


Fig. 3 Throughput vs. the number of packets per second.

Fig. 3 shows that PDM with $h(n_{Sp}\text{-}n_{Dp})$=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.

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. Thus 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 as the attacker forwards many data packets at a high rate for the whole session. Many users like to download and share multimedia data. Therefore we expect that the proposed scheme is useful to networks where burst traffic is transferred.

REFERENCES

1. A. Jamalipour, "Self-organizing networks ,"*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 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. AlShurman, 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.