Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.134 – 138

RESEARCH ARTICLE

Defending Against Attack in Heterogeneous Networks

M. Mukesh Krishnan
II M.E – Computer Science Engineering,
Francis Xavier Engineering College,
Tirunelveli, Tamilnadu
mukeshkrishnan.m@gmail.com

R. Ravi
M.E., Ph. D, Professor and HOD
Department of CSE,
Francis Xavier Engineering College,
Tirunelveli, Tamilnadu

***Abstract:** In Disruption Tolerant Network flood attack is occur when the packets or packet replicas are send continuously from source to destination. Flood attack normally cause packet loss and inconsistency in packets. In order to overcome flood attack rate limit has been set in each node so the nodes only accept the particular limit of data's. Our detection adopts Claim-carry-and check in which each node itself counts the number of packets or replicas that it has sent and claims the count to other nodes. When the node violates its rate limits, it will be detected and its data traffic will be filtered by the way the amount of traffic has to be reduce. The receiving nodes carry the claims when they move and cross-check if their carried claims are inconsistent when they contact. To avoid this data loss we propose a technique Distributed Dynamic Routing Algorithm. This algorithm provides the best path in a network to perform effective communication dynamically. The Distributed Dynamic Routing Algorithm chooses a best path to transmit data from source to destination through intermediate nodes randomly. Here the network posse's parallel communication so the transmission time is very low. Since the protocol transmits data randomly data transmission is more secure. Since the data's send dynamically the communication is efficient without any malicious activity.*

Index Terms—DTN; security; flood attack; DDR; CCC; detection

I. INTRODUCTION

A specialized field in computer networking that involves securing a computer network infrastructure. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have easy access to the network and resources to work. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network. The main purpose is to secure the data and files from the unwanted access from the network and other items.

© 2014, IJCSMC All Rights Reserved

II. SYSTEM ANALYSIS

A. Problem Definition

The problem is rely on some kind of inconsistency in network when communicating data from source to destination and they do not handle long delays of detection. The activity of DTN is get monitor in the gateway and detects the deviations in the expected behaviour. In previous study Claim-Carry-and check was used. In this approach each node has limit over number of packets that it can send or accept from source node in particular time interval and each node has number of replicas that it can generate for each packet. If a node violates its rate limits, it will be detected and its data traffic will be filtered by the way, the amount of flooded traffic can be controlled.

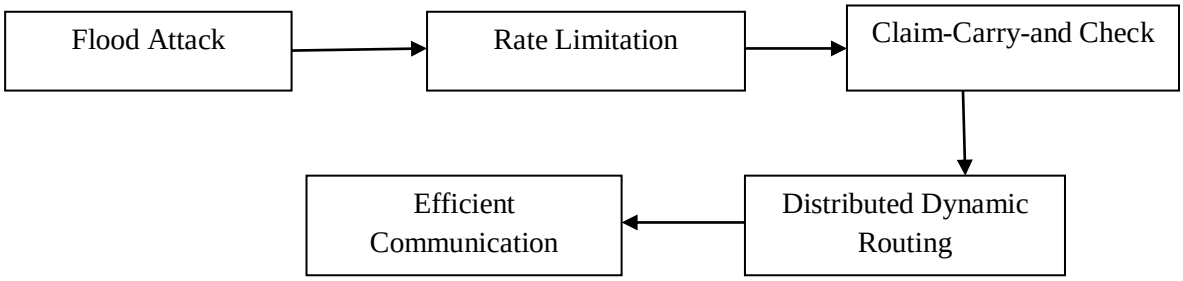
B. Existing System

In WIRELESS sensor networks, nodes have limited energy resources and protocols designed for sensor networks should be energy-efficient. In existing approach claim-carry-and check has been used in which each node has limit over number of packet that it has send to destination and accept from source node in particular interval of time and each node has limit over number of replicas that it can generate for each packet. When the node violates its rate limits, it will be detected and its data traffic has to be filter. Even though on using Claim-carry- and check technique there is some data loss and data transmission time is too late to reach the destination.

C. Proposed System

In DTN the packet send efficiently to its destination by sending each packet dynamically in distributed path. Distributed Dynamic Routing algorithm is used to send packet dynamically in distributed manner and due to this algorithm data loss has been reduced and this algorithm provides the best path in a network to perform effective communication dynamically. The Distributed Dynamic Routing Algorithm chooses a best path to transmit data from source to destination through intermediate nodes randomly. It possess parallel communication. Since this protocol uses parallel communication, the transmission time is very low and this protocol transmits data randomly, the data transmission will be more secure.

III. SYSTEM ARCHITECTURE



IV. SYSTEM MODULES

A. Network Construction

Topology creation is creating a network and maintaining communication among various nodes in peer to peer network which helps us to share the data. In the network, numerous nodes are interconnected and exchange data or services directly with each other. To create a new node the node name, IP address, and port address for data communication has to mention. When the entire node successfully then connection is needed to establish to create the network.

B. Rate Limitation

Every node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. Each node also has a limit over the number of replicas that it can generate for each packet. The two limits are used to mitigate packet flood and replica flood attacks, respectively. If a node violates its rate limits, it will be detected and its data traffic will be filtered. In this way, the amount of flooded traffic can be controlled.

© 2014, IJCSMC All Rights Reserved

C. Claim-Carry-and Check

In Claim- Carry-and Check each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes. Each node also has a limit over the number of replicas that it can generate for each packet. The counted node is mention on the packet head beyond the entire packet. Based on the behavior of the destination node the source performs further packet transmission. Since the packet on the particular path is reach its destination dynamically the data loss is get reduced.

D. Distributed Dynamic Routing

The Distributed Dynamic Routing algorithm is designed to provide the best path in a network to perform effective communication dynamically. It chooses a best path to transmit data from source to destination through intermediate nodes randomly. It posses parallel communication.

E. Effective Communication

The data can be communicated effectively without any malicious activity. The rate limiting to defend against flood attacks in DTNs and hence the data is transferred to the destination more effectively. So the communication is made more effective without the attack of malicious node in the network.

V. ALGORITHM

A. Distributed Dynamic Routing Algorithm

This algorithm provides the best path in a network to perform effective communication dynamically. The Distributed Dynamic Routing Algorithm chooses a best path to transmit data from source to destination through intermediate nodes randomly. It posses parallel communication between various intermediate nodes. The distributed dynamic routing directs packet forwarding (that transit of logically addressed network packets from their source toward their destination) through intermediate nodes. This routing technology is used to select the best path among various nodes in the network and forwards the packets through the selected path dynamically. Hence the communication between intermediate nodes are more efficient.

B. *Sender*

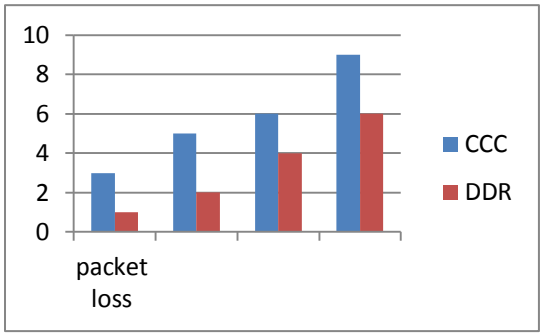
```
begin
accept large packet;
if largepacket <=48
begin
find the free channel;
send largepacket;
end
else
begin
no: of packets= largepacket/48;
send the no: of packets;
for(i=0; i<=no: of packets;i++)
begin
P[i] = largepacket-[largepacket-48];
find the free channel;
send p[i];
end
loop end
end
end if
end
```

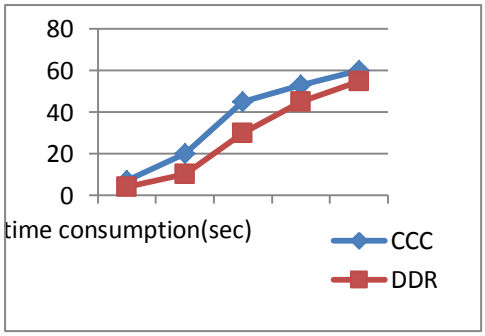
C. *Receiver*

```
begin
receive no: of packet;
for(i=0; i< no: of packet; i++ )
begin
```

© 2014, IJCSMC All Rights Reserved

```
receive(p[i]);
r[i]=p[i];
end
end loop
for(i=0; i< no: of packet; i++)
begin
for(j=0; j<no: of packet-i-1;i++)
begin
if(r[j]>r[j+1])
begin
temp=r[j];
r[j]=r[j+1];
r[j+1]=temp;
end
end if
end
end loop
for(i=0;i<no: of packet; i++)
begin
receivedpackets = 0;
receivedpackets = receivedpackets+r[i];
end
end loop
end
```





VI. CONCLUSION

To evaluate the performance of cooperative transmission, where nodes in a sending cluster are synchronized to communicate a packet to nodes in a receiving cluster. In the communication model, the power of the received signal at each node of the receiving cluster is a sum of the powers of the transmitted independent signals of the nodes in the sending cluster. The increased power of the received signal, vis-à-vis the traditional single-node-to-single-node communication, leads to overall saving in network energy and to end-to-end robustness to data loss. Similarly, compared to the CAN protocol and to the one-path scheme, this reduction amounts to a factor of up to 10,000. The total energy consumption was analytically computed, illustrating substantial energy savings. For example, when nodes are positioned on a grid, the energy savings of the cooperative protocol over the CAN protocol is up to 80%. The size of the clusters, should be relatively small, when the inter-cluster distance is small, with the optimal value of increasing with . For scenarios that are not covered by the theoretical analysis, uses simulation to evaluate and compare the protocols. For random placement of nodes, the simulation results show that the cooperative transmission protocol saves up to 20% of energy compared to the CAN protocol and up to 40% of energy compared with the disjoint-paths and the one-path scheme.

REFERENCES

1. Daly.E and Haahr.M (2007), 'Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs',Proc. MobiHoc, Vol. 18,No. 7,pp. 32-40.
2. Fall(2003), 'A Delay-Tolerant Network Architecture for Challenged Internets',ACM SIGCOMM, Vol. 22 ,No. 5, pp. 27-34.

© 2014, IJCSMC All Rights Reserved

3. Grid.S.J.T.U Computing Center(2012), 'Shanghai Taxi Trace Data',http://wirelesslab.sjtu.edu.cn ,Vol. 19,No. 8, pp. 32-43.
4. Gao.W, Li.Q, Zhao.B, and Cao.G (2009), 'Multicasting in Delay Tolerant Networks: A Social Network Perspective',Proc. ACM MobiHoc,Vol. 12,No. 6,pp. 42-49.
5. Gao.W, Cao.G, Srivatsa.M, and Iyengar.A(2012), 'Distributed Maintenance of Cache Freshness in Opportunistic Mobile Networks', IEEE ICDCS, Vol. 11,No. 9,pp. 27-33.
6. Groenevelt.R(2006), 'Stochastic Models in Mobile Ad Hoc Networks',technical report, Univ.of Nice, Sophia Antipolis, INRIA, Vol. 12,No .7,pp. 34-39.
7. Hui.P, ChaiScott.A, Gass.R, Crowcroft.R, and Diot.S,(2005),'Pocket Switched Networks and Human Mobility in Conference Environments',Proc. ACM SIGCOMM, Vol. 21, No. 6, pp. 21-33.
8. Li.Q and Cao.G(2012),'Mitigating Routing Misbehavior in Disruption Tolerant Networks', IEEE Trans. Information Forensics and Security, Vol. 7, No. 2, pp. 45-56.
9. Li.Q, Gao.W, Zhu.S, and Cao.G (2012), 'A Routing Protocol for Socially Selfish Delay Tolerant Networks', Ad Hoc Networks,Vol. 10, No. 8, pp. 26-32.
10. Mirkovic.J, Dietrich.S, Dittrich.D, and Reiher.P(2005), 'Internet Denial of Service: Attack and Defense Mechanisms', Prentice Hall, Vol. 21,No. 4, pp. 27-36.
11. Motani.M, Srinivasan.M, and Nuggehalli.P(2006),'PeopleNet: Engineering a Wireless Virtual Social Network',Proc. MobiCom, Vol. 23, No. 4,pp. 243-257.
12. Ren.Y, Chuah.M.C,Yang.J, and Chen.Y(2010),'Detecting Wormhole Attacks in Delay Tolerant Network",IEEE Wireless Comm.Magazine, Vol. 17, No. 5, pp. 36-42.
13. Shevade.U, Song.H, Qiu.L, and Chen.Y(2008), 'Incentive-Aware Routing in DTNS', Proc. IEEE Int'l Conf. Network Protocols(ICNP'08), Vol. 17,No. 5,pp. 32-41.
14. Srinivasan.F, Li, A. and Wu.J(2009),'Thwarting Blackhole Attacks in Distruption-Tolerant Networks Using Encounter Tickets', Proc.IEEE INFOCOM, Vol. 13,No. 8, pp. 31-38.

AUTHORS PROFILE

M.Mukesh Krishnan is presently studying M.E second year Computer Sciences and Engineering in FrancisXavier Engineering College. He has completed his B.E Computer Science and Engineering from Einstein College of Engineering. His field of interests are Network Security, Computer Applications in Network Security..

R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has completed his Ph.D in Networks from Anna University Chennai. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

Dr. Beulah Shekhar is a Coordinator for Victimology & Victim Assistance, in the Department of Criminology and Criminal Justice Sciences; she is presently working as a Associate Professor in the Department of Criminology and Criminal Justice Sciences. And her areas of interest are Crimes against Women Empowerment, Human Rights, and Police Training.

© 2014, IJCSMC All Rights Reserved