Design and Implementation of Chord Algorithm in Wireless Mesh Networks

K. Sharath Kumar[#1],
[#]Associate Professor, Dept. of CSE,
Sphoorthy Engineering College
Hyderabad, Telangana, India

Dr. M. Rama Bai*2
[*]Professor & Head, Dept. of IT, MGIT
Gandipet, Hyderabad, Telangana, India

Abstract-We detect, identify and evaluate the epidemic attackers that are cruel node which generate polluted packets in wireless mesh networks (WMNs). Epidemic attack is a severe protection problem in network-coding enabled WMNs. These allow the presence of smart attackers, i.e., they can transmit valid packets so as to reduce the chance of being detected. It also addresses the case where attackers cooperatively inject polluted packets. It employs the time-based checksum and batch verification to determine the existence of polluted packets, and then propose a set of chord algorithms so that each legitimate node in a WMN can identify its malicious neighbours. It provides formal analysis to quantify the performance of the algorithms. Here it will occur a time consuming process based on checksum. In proposed system it removes the unwanted checksum in intermediate nodes based on arrival of data from source node using TTL. It shows the effectiveness and efficiency of the detection algorithms. The result is soon in simulations.

Index Terms: Epidemic Attack, Wireless Mesh Networks, Network Coding, Efficiency improvement

I INTRODUCTION

Network security consists of the provisions and polices adopted a network administrator to prevent and monitor unauthorized access, misuse, modification, or denunciation of a system network and network-accessible assets. Network safety measures involve the approval of access to data in a set of connections, which is controlled by the system administrator. Users are assigned a identification and key or other authenticating information that allows them access the information and programs within their right. System security covers a variety of PC networks, both public and private, that are used in everyday jobs conducting and communicating surrounded by businesses, management agencies and persons. Networks can be confidential, such as within a business, as well as others which might be open to community access. System security involved in group endeavour, and additional type of institution. The most common and simple way of shielding a set of connections resource is by assigning it a unique name and a corresponding password. Network security starts with authenticating commonly with a username and a password. It requires just individual detail authenticating the user name & password this is sometimes termed one-factor authentication.

Wireless mesh networks (WMNs) have emerged as a promising platform to provide easy Internet access [5] I. Akyildiz Et al described that however, due to the spatial and temporal fading of the wireless channel, message links between nodes usually have high loss rates. As reported in, half of the operational links have a loss probability greater than 30%. Therefore, traditional steering protocols, which establish the next hop in forwarding a packet, cannot assurance a high end-to-end throughput. We have seen some exciting advancements in wireless routing protocols to improve the performance of WMNs. One such protocol that is receiving a lot of attention is the opportunistic routing protocol. In this protocol, any node which overhears the transmission of another node can participate in data forwarding. Using this hypothesis, high end-to-end communication can be obtained even if some links along the source-destination path are glossy. However, since multiple nodes which overhear the packet can participate in the data forwarding, packet conflict may occur and thereby reduces the network capacity.

Infrastructure / Backbone WMNs. In this construction, mesh routers form a road and rail network for patrons, where dashed and solid lines indicate wireless and wired links, respectively. Infrastructure/backbone can be built using various types of radio technology, in adding together to the mostly used IEEE 802.11 technologies. The interconnect routers form a mesh of self-configuring, self-healing links among themselves. Conventional clients with an Ethernet interface can be connected to mesh routers via Ethernet associates. For predictable clients with the same radio technologies as mesh steering, they can directly correspond with mesh routers

Client WMNs. Client meshing provides peer-to-peer networks among user devices. In this type of design, client nodes represent the genuine network to perform routing and construction functionalities as well as providing end-user applications to clients. Hence, a mesh router is not required for these types of networks.

Hybrid WMNs. Mesh clients can access the network through mesh routers as well as directly meshing with other interconnect clients. While the road and rail network provides connectivity to other networks such as the

Internet, wireless network, cellular, and sensor networks, the steering capabilities of clients provide improved connectivity and coverage area inside WMNs.

In this concept the epidemic attackers are identified and evaluated by using the Packet generation and using the checksum of the nodes. The chord algorithm is used which defines the node id were the attackers can be identified and when the collision occur the Load balancing concept is used.

2. RELATED WORKS

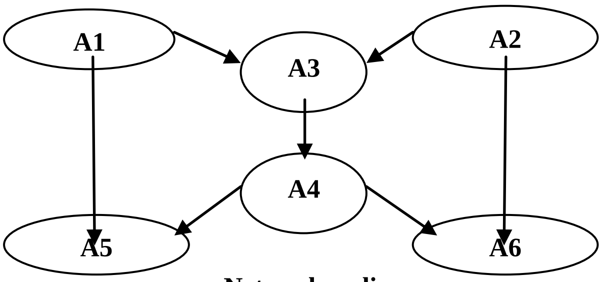
A core problem in WMNs is attackers mainly the epidemic attackers. A particular paradigm for this attack is due to the pollution of data in network while, forwarding the data from source to the destination the attacker act as the malicious node and do the process.

2.1 Network Information Flow

The network coding defines the flow of the data in the network when we are using this technique as the paradigm. Point-to-point communication network [16] R. Ahlswede Et al determined that on which a number of information sources are to be multicast to certain sets of destinations. We guess that the information sources are commonly independent. The difficulty is to characterize the permissible coding rate region. This replica subsumes all earlier studied models along the same line. Source nodes multicast information to other nodes on the network in multi hop fashion [3] S.-Y. R. Li Et al described where every node can pass on any of its received data to others. Here the problem arries whether optimization of the multicast mechanisms at the nodes. Prove that linear coding suffices to reach the finest; which is the max-flow from the source to each receiving node. The code constructed is not the simplest possible Construction of a code for multicast in a network that achieves the max-flow bound on the information transmission rate.

2.2 Link-level Measurements

Describes the packet loss in a 38-node urban multi-hop 802.11b network [2] D. Aguayo Et al determined the patterns and causes of loss are important in the design of routing and error modification protocols, as well as in network planning. The distribution of inter-node loss rates is relatively uniform over the whole range of loss rates; there is no clear threshold separating "in range" and "out of range."The attackers are detected by using the routing protocol which do not provide the efficient finding of the malicious node within the time randomized algorithm is one method used by [1] Yongkun Li Et al determined this method..



Network coding

2.3 Wireless mesh routers

Wireless mesh networks (WMNs) typically consist of mesh routers and mesh clients with each node having the capability of operating not only as a host but also as a router.[3] S.-Y. R. Li Et al described based on the functionality of the nodes, WMNs can be classified into three categories: Infrastructure backbone, client backbone and hybrid [5] I. Akyildiz Et al described mesh routers are used to form a multi-hop and multi-path wireless relay backbone capable of communicating with gateways and clients. Other than the routing capability for gateway/bridge functions as in a conventional wireless router, a interconnect router contains extra routing functions to support mesh networking. Through multi-hop interactions, the same reporting can be achieved by a mesh router with much lower transmission power. The underlying techniques exploit space diversity available through cooperating terminals relaying signals for one another. Outlined several strategies employed by the cooperating radios, including permanent relaying schemes such as amplify-and-forward and decrypt-and-forward, choice relaying schemes that adapt based upon channel measurements between the adjustable terminals, and improvement relaying schemes that adapt based upon limited feedback from the destination terminal. Developed performance characterizations in terms of outage events and associated outage probabilities, which measure toughness of the transmissions to declining, focusing on the high signal-to-noise ratio (SNR) regime [4] J. N. Laneman Et al which describes that this paper has the variety of low-complexity, supportive procedure that enable a pair of wireless terminals, each with a particular antenna, to fully develop spatial range in the channel.

2.4 Random Network Coding

An information-theoretic approach for detecting Byzantine [6] M. Siavoshani Et al analyzed the adversarial modifications in networks employing random linear network coding is described. Each exogenous foundation packet is amplified with a bendable number of hash symbols that are obtained as a polynomial function of the data symbols. They identify two general frameworks that encompass several network coding-based systems proposed for unicast in wireless networks [7] T. Ho, B. Leong Et al covered the above method.

3. DATA TRANSFER USING PACKET GENERATION

Construct a network which consists of 'n' number of nodes. Network is the module which is used to store all the Nodes information like Node Id, checksum, buffer level and TTL. Also the network will monitor all the Nodes communication for security purpose. If a node send data to destination node means source node first give a request to network for identifying active nodes. After identification active nodes then network find out intermediate nodes based on source node using shortest path algorithm. Identification shortest path is used to reduce cost and time. Node establishes their routing protocol to the nearest nodes using the shortest path algorithm. The multiple paths will be found for data transmission. But the path with minimum no. of hops (nodes) only elected for the data transmission. Source node has lot of packets. So it separate the packets based on capacity. It is used for quick data transfer. So it reduces the packet loss in intermediate nodes. For example suppose source node has 5MB data means it separate that data in to lot of packets based on packet generation.

4. ATTACK DETECTION

The attack is detected by using the set of algorithms. First the data is divided in to the number of generations as described earlier and to detect the attacker the chord algorithm is used, it can verify the Neighbour nodes information of the Requested Node like Predecessor Node Id with content and Successor Node Id with content. These are verifying the Node Id's and Location Id's then we can detect the Attacker Node. For this purpose we have to create the list of the neighbour nodes information for each node so that the Intermediate Node can verify the nodes request.

4.1 Encryption Methodology

Packet encryption is done by the normal method like plain text and cipher text in order to provide more secure packet transmission from source to destination the signcryption methodology is proposed for encryption. The signcryption methodology provides both digital signature as well as encryption. It provides the formal mathematical formulations scheme.

5. BUFFER LEVEL USING LOAD BALANCING ALGORITHM

It is used to identify the time based on arrival of data. So each intermediate node has checksum using TTL(time to live). It also used to identify the hacker based on data arrival in the intermediate node. The checksum fix some amount of time for data transfer to another node. For example intermediate node transfer data before checksum is complete means checksum receives another source node data for transmission. In this phase we maintain a buffer level of each intermediate node. The buffer level has two types i.e., unverified buffer and verified buffer. Unverified buffer receives data from source node then only data goes to verified buffer. Unverified buffer also has total generation, current generation, total packet, current packet, node id on particular source node. Then the verified buffer checks the all information of data then only data reaches the destination node. Load balancing algorithm also used for unverified buffer. Because data is holding on unverified buffer based on same time another data is received on that buffer. The unverified buffer sends the holding data in to another active intermediate node for reaching destination. It is used to minimize the time consumption.

6. PERFORMANCE EVALUATION

Figure.1 shows the secure packet delivery from the source to the destination. The throughput is obtained by using the network coding i.e., the packet generation were each packet is divided in to the generation were each generation consists of n number of packets. For example if the total size of the data is 10mb then it is further split in to the generations and the data is transmitted. The shortest path is identified by the source so that the data reaches the destination correctly. The throughput is increased by the methodology of network coding, shortest path selection and the neighbour list identification. The performance of the packets reaching the destination is increased in the proposed system compared to that of the existing system.

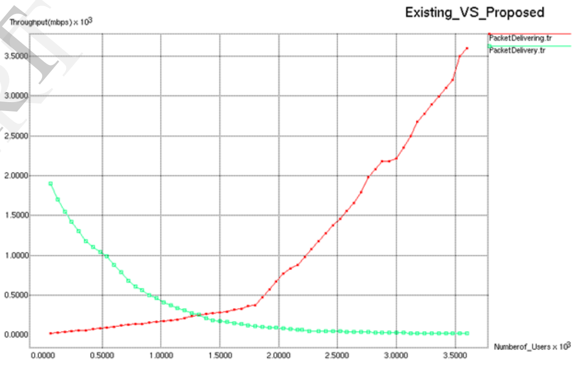


Fig. 1 packet delivery

In the above simulation we have shown the performance of the algorithm which is used. When the multiple attackers take place the malicious node is detected, is shown in the simulation. The encryption is used for the packet delivery. It defines the secure packet delivery were the attacker will not be able to view the data. The performance is further increased by encryption of the plain text and cipher text along with the digital signature. This enables the packet delivery upon the nodes were each node cannot view the data. The figure.2 shows the result of the simulation which analyzes the delay and detection of the attackers.

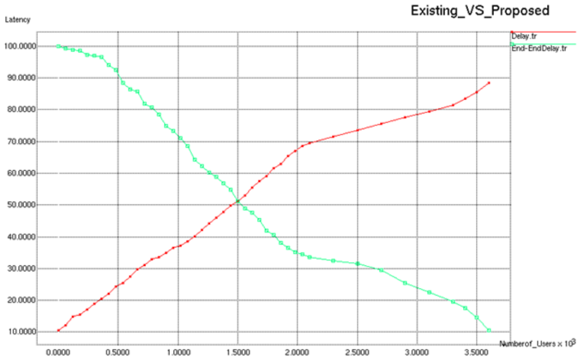


Fig.2 Attacker Detection and end to end delay analyzes

The chord algorithm is used to verify the Node Id's and Location Id's, then we can detect the Attacker Node. For this purpose we have to create the List of the Neighbour Nodes information for each node so that the Intermediate Node can verify the nodes request i.e., unverified and the verified buffer is used, when the attacker is identified they are further informed to all other nodes and no data passes through that node. When the delay occur the Load balancing algorithm is used which eliminate the collusion/delay. The energy level of each node is maintained using that the malicious node is identified and eliminated. The comparison between the existing and the proposed is shown in both the figures. The theoretic approach is shown in the result of the simulation which provides the exact performance of each methodology. We show the effectiveness and efficiency of the algorithms in the form of the simulation. Fig.3 shows the comparison of the existing vs proposed time consumption.

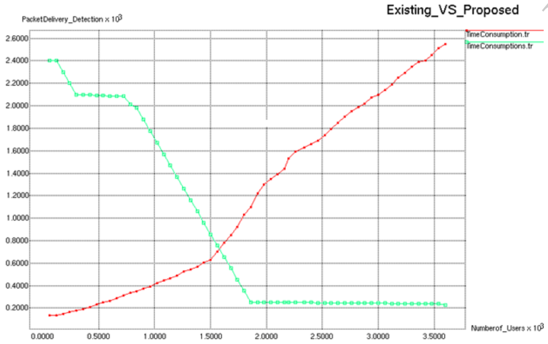


Fig. 3 Time consumption

The time consumption of the packet delivery is reduced is proposed. Fig. 4 Shows the overall performance of each schemes proposed. The energy level of the each node exists the level then the attackers are detected and they are further delectated. The result shown defines the level of the energy maintained as defined. If the energy exists i.e., less than the 30 j the malicious node is identified which acted as the legitimate node. The analyzer defines the attacker detection of multiple as well as the single node.

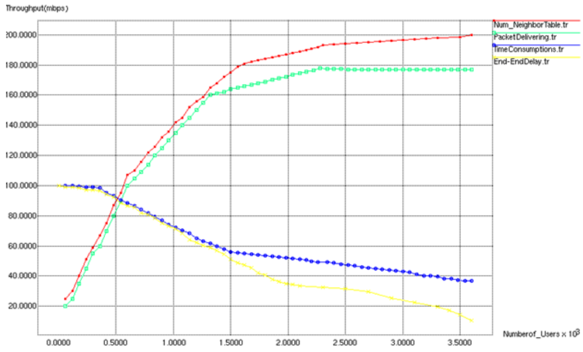


Fig. 4 Detection methodology

7. CONCLUSION

In this Paper, a set of fully distributed defense and detection algorithms to address the pollution attack problem in wireless mesh networks which are configured with network coding enabled opportunistic routing protocol. The contribution of this Paper is on how to effectively discover the malicious nodes without modifying existing routing protocol and packets verification scheme, and then isolate them from the network so as to defend against the pollution attack. We consider both cases where malicious nodes always forward polluted packets, and the malicious nodes may pretend to be legitimate nodes and forward valid packets so as to evade the detection. It also uses load balancing algorithm in buffer level. So it also speeds up the detection. It provides formal analysis to quantify the performance of our detection algorithms, and extensive simulations are provided to validate the theoretic analysis and show the effectiveness and efficiency of the detection algorithms.

8. REFERENCES

[1] Epidemic Attacks in Network-Coding Enabled Wireless Mesh Networks: Detection, Identification and Evaluation Yongkun Li and John C.S. Lui, Fellow, IEEE, Fellow, ACM

[2]D. Aguayo, J. C. Bicket, S. Biswas, G. Judd, and R. Morris. Link-level Measurements from an 802.11b Mesh Network. In SIGCOMM, pages 121–132, 2002.

[3] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear Network Coding. IEEE Transaction on Information Theory, 49(2):371–381, Feb. 2003.

[4] J. N. Laneman, D. N. C. Tse, and G. W. Wornell. Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. IEEE Transactions on Information Theory, 50(12):3062–3080, December 2004.

[5] I. Akyildiz and X. Wang. A Survey on Wireless Mesh Networks. IEEE Radio communication, 43(9):S23–S30, September 2005.

[6] M. Siavoshani, C. Fragouli, and S. Diggavi. On Locating Byzantine Attackers. In Network Coding, Theory and Applications,2008.

[7] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. Karger. Byzantine Modification Detection in Multicast Networks with Random Network Coding. Information Theory, IEEE Transactions on, 2008.

[8] S. Vyetrenko, A. Khosla, and T. Ho. On Combining Information theoretic and Cryptographic Approaches to Network Coding Security against the Pollution Attack. In 2008 IEEE Transactions.

[9] J. Dong, R. Curtmola, R. Sethi, and C. Nita-Rotaru. Toward Secure Network Coding in Wireless Networks: Threats and Challenges. Secure Network Protocols, 2008.

[10] P. Bahl, R. Chandra, P. P. C. Lee, V. Misra, J. Padhye, D. Rubenstein, and Y. Yu. Opportunistic Use of Client Repeaters to Improve Performance of WLANs. ACM, New York, NY, USA, 2008.

[11] J. Dong, R. Curtmola, and C. Nita-Rotaru. Practical Defenses against Pollution Attacks in Intra-flow Network Coding for Wireless Mesh Networks. In WiSec '09: of the ACM..

[12] J. Le, J. C. S. Lui, and D.-M. Chiu. Dcar: Distributed Coding- Aware Routing in Wireless Networks. IEEE Transactions on Mobile Computing, 9:596–608, 2010.

[13] Tan Le, Yong Liu [2010]," On the Capacity of Hybrid Wireless Networks with Opportunistic Routing". IEEE Transactions on Mobile Computing, 9:596–608, 2010.

[14] S. Biswas and R. Morris. Opportunistic Routing in Multi-hop Wireless Networks. SIGCOMM Comput. Commun. Rev., 34(1):69–74, 2011.

[15] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *J. ACM*, vol. 40, no. 1, , Jan. 1993.

[16] R. Ahlswede, N. CAI, S.-Y. R. Li and R.W. Yeung. Network Information Flow. IEEE Transactions on Information Theory, 46(4):1204–1216, July 2000.

Authors:

Mr.K.Sharath Kumar received, his B.Tech(CSE), from Pondicherry University, Puducherry and his M.Tech (CSE) from Bharath University, Chennai (TN). He is a research scholar at JNTUH, Hyderabad. He is currently working as Associate Professor in Sphoorthy Engineering College, Hyderabad, Telangana. He is a Life Member in ISTE. His area of interests includes, Image Processing, Software Engineering, Wireless Network Security and Database Systems. He has published papers in international journals and national conferences.

Dr. M. Rama Bai received, her B.E degree from Bharathiar University, Coimbatore(T.N) and her M.Tech (CSE) from College of Engineering, Osmania University, Hyderabad. She received her Ph.D. degree in Computer Science from Jawaharlal Nehru Technological University, Kakinada(JNTUK) in 2012. She served Amrita University, Coimbatore and Sri Hindu College of Engineering, Machilipatnam before joining in MGIT for some period. She then joined as Assistant Professor in the Dept of Computer Science & Engineering, Mahatma Gandhi Institute of Technology (MGIT) in1999. At present she is working as Professor in Dept of CSE, MGIT. Her research interests include Image Processing, Pattern Recognition, Digital Water Marking and Image Retrieval Systems. She has published 18 research publications in various National and International Journals and conferences.