RESEARCH ARTICLE OPEN ACCESS

Literature survey on Security Analysis in Multi-hop Wireless Networks

P.Gnana prakash[1], Dr. P.Rajkumar[2]
M.E1, Assistant Professor2, Dept. of Computer Science and Engineering,
Info Institute of Engineering, Coimbatore, TamilNadu-India
Anna University Chennai

ABSTRACT
Multi-hop wireless networks are the type of networks which require two or more wireless hops to deliver the information from the source to destination. The security in multi-hop wireless networks is the major challenge. The most of the routing algorithm has the insecure data transfer in nature. In this paper, we aim to identify the security measures that could increase the security of routing protocol. The several algorithms are used to increase the security as well as performance in the data transfer on multi-hop wireless networks.
***Keywords*- N**etwork coding, GEV, NRP, Routing, Multicasting.

I. Introduction

In the year 2009 X.Lin proposed Routing is the technique used to move a data packet from the sender to receiver. It enables the messages to pass from one node (computer) to another leading it to finally reach the destination. Every data packet contains within it the set of information including what is it, where it is coming from (sender's IP address) and where it is going (receiver's IP address) *Ref[2]*.

The device called as router is used to perform routing in a network. While we consider routing in Multi-hop wireless networks, it becomes immensely necessary to find the optimal and most secure routing protocols out of the existing ones. The aim of our study is to secure these multi-hop wireless network protocols *Ref [2]*. We have tried to first discuss the various routing protocols and various security attacks on these routing protocols. Then after discussing attacks on routing protocols, we have identified the security measures that could help to increase the reliability of the protocols.

II. Routing in multi-hop wireless networks

Opportunistic routing is based on the use of broadcast transmissions to expand the potential forwarders that can assist in the retransmission of the data packets. The receptors need to be coordinated in order to avoid duplicated transmissions. This is usually achieved by ordering the forwarding nodes according to some criteria. The proposed opportunistic routing protocols differ in the criterion to order the receptors and the way the receptors coordinate. This paper presents a survey of the most significant opportunistic routing protocols for multi-hop wireless networks. *Ref [5]*.

Opportunistic routing protocols present a promising scheme to improve the wireless network performance by exploiting the broadcast nature of the medium. The main concern of theses protocols relies on which neighbouring nodes should forward the data packets and how to coordinate them to avoid duplicated retransmissions. The way to select the relays is supported by metrics. This paper has reviewed the main proposals for multi-hop ad hoc networks and we have classified them according to the kind of metric used. *Ref [2]*.We can see that the geographic and link-quality based routing protocols have been extended by coding opportunistic routing protocols.

III. Network Coding Algorithm

We consider multicast communications from a single source to multiple destinations through a wireless network with unreliable links. Random linear network coding achieves the minuet flow capacity; however, additional overhead is needed for end-to-end error protection and to communicate the network coding matrix to each destination. We present a *joint coding and training* scheme in which training bits are appended to each source packet, and the channel code is applied across both the

training and data. This scheme allows each destination to decode jointly the network coding matrix along with the data without knowledge of the network topology. It also balances the reliability of communicating the network coding matrices with the reliability of data detection.

The throughput for this scheme, accounting for overhead, is characterized as a function of the packet size, channel properties (error and erasure statistics), number of independent messages, and field size. We also compare the performance with that obtained by individual channel coding of training and data. Numerical results are presented for a grid network that illustrates the reduction in throughput due to Overhead. *Ref [2]*.

IV. Attacks on multi-hop wireless networks.

The multi-hop wireless networks are wireless are widely accepted and its applications are increasing day by day. But the security of these networks is becoming a major key challenge in the wide-scale deployment of these networks. In simple and general context, an adversary is one's opponent in a contest, conflict or dispute. In the term of wireless network, an adversary is a node that opposes or attacks the security of the network and leading to an insecure communication in the network. These security attacks aim to increase the control of these adversary nodes over the communication between some nodes in the network. These attacks tend to degrade the quality of the network services and also increase the resource consumption. Adversaries are not physically present but aim to corrupt the legitimate nodes by launching attacks from regular devices. *Anurag Joshi2*,(2009).

4.1 Types of Attacks

The various types of security attacks are listed below:

1. Route disruption
2. Route diversion
3. Creation of incorrect routing state
4. Generation of extra control traffic
5. Creation of a gray hole

4.1.1 Route Disruption.

In the route disruption attack the adversary prevents a route from being discovered between two connected nodes. The main objective of this attack is to degrade the quality of network services. The two connected nodes cannot communicate directly and therefore a route is followed that has the adversarial control. **The attack mechanisms are:**

1. Dropping of Route Request or Route Reply messages.
2. Forging route error messages.
3. The dropping of control packet.
4. Wormhole attack.

4.1.2 Route Diversion.

Route diversion attack leads to the establishment of the routes which are different from the ones that the protocol would establish due to the interference of the adversary. The adversary aims to achieve that the diverted routes should have its control over the link so that it can eavesdrop or modify the data that is been sent between the victim nodes. It also has side effects of increase in resource consumption, overloading the network links and delay in the delivery of the data. The attack mechanisms are:

1. Modifying or dropping control messages
2. Setting up a wormhole/tunnel

4.1.3 Creation of incorrect routing states.

In this attack, the insecure and adversary nodes are appeared to be secure and the state appears to be correct but in fact they are not. So when the data packets are routed using the infected state they never reach their desired destination because of these corrupted nodes. This can be achieved by modifying, spoofing, forging or dropping of control packets.

4.1.4 Generation of extra control traffic.

This attacks aims at injecting spoofed control packets into the networks. Spoofing is the technique of masquerading others by modifying or falsifying data resulting in gaining illegitimate advantage. It leads to the

increase in consumption of resources by flooding the illegitimate control packets in network.

4.1.5 Setting up a Gray Hole.

Gray hole [9] attacks the network by leading the nodes to drop the packets selectively. This attack leads to the data to be either malicious or unnecessary by dropping all UDP packets while forwarding TCP packet or by dropping packets by probabilistic distribution. Gray hole is actually an attacker node but behaves as a correct one. Therefore, it becomes very difficult to identify the attacker node in the network.

V. Securing multi-hop wireless network routing protocol (NRP).

After discussing several attacks that could degrade the quality of the network, we aim to list out various security countermeasures and algorithms that could help to increase the security and prevent these attacks.

Kritika Jain, Anurag Joshi, Pawan Prakash,(2009).

5.1countermeasures.

1. Authenticating control packets
2. Protection of mutable information in control packets
3. Reducing gray holes from the network

5.1.1 Authentication of control packets.

In the network whenever a packet is transmitted it has two sets of information: control information and user data often called as payload. the control information contains the source and destination addresses, checksums and sequence information. The adversaries often attack the control information of the packet in order to degrade the quality of service. Control packets should be authenticated by the initiators of the packet using Message Authentication Code and the authenticity should be verifiable by the destination node. For example Ariadne which is used to secure the basic version of DSR algorithm .Now when this packet reaches any intermediate node, that node must be able to verify its authenticity before processing the control packet. After the verification, the intermediate nodes update their routing state. A Broadcast Authentication scheme must be employed to verify the authenticity of the nodes.

5.1.2 Protection of Mutable Information in Control Packets.

There are certain set of inconstant information that can be altered or changed throughout the network. This mutable information (hop count, node list etc) is added by intermediate nodes to the control packets before forwarding it. Since this information is not protected, the adversary could easily attack and modify making it malicious. To prevent this, each intermediate node before entering or modifying this mutable information should verify its authenticity. If the node is found authenticated to enter or modify the information then only it is liable to alter any information.

5.1.3Combating Gray Holes

Gray holes are very difficult to detect in a network. It is much easier to deal with an attacker rather than detecting it out of the correct nodes. In order to reduce these gray holes, multiple routes should be traced out to deliver a data packet. It would be preferable if these routes are Node Disjoint paths [10] Node Disjoint Paths reduces routing overhead and also provides robustness to mobility. To decrease the resource consumption, the data packet should be coded and then break up into smaller chunks. If a threshold value is set for the number of chunks then it will prove beneficial to the network. Then these chunks of packet are sent over different routes on entire network.

5.2 algorithms

1. Novel network coding.
2. Global Encoding Vectors (GEVs)

5.2.1 Novel network coding

Consider a communication network in which certain source nodes multicast information to other nodes on the network in the multi-hop fashion where every node can pass on any of its received data to others. We are interested in how fast *each* node can receive the complete information, or equivalently, what the information rate

arriving at *each* node is. Allowing a node to encode its received data before passing it on, the question involves optimization of the multicast mechanisms at the nodes. Among the simplest coding schemes is linear coding, which regards a block of data as a vector over a certain base field and allows a node to apply a linear transformation to a vector before passing it on. We formulate this multicast problem and prove that linear coding suffices to achieve the optimum, which is the max-

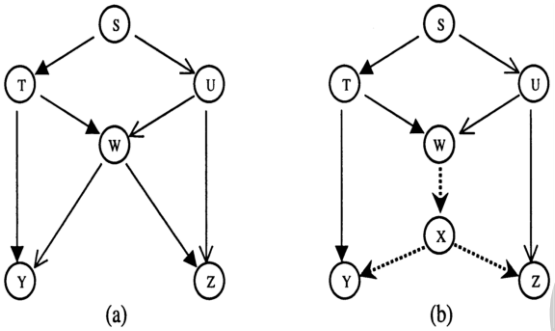

Fig1. Two Communication Networks.

Flow from the source to each receiving node. *Shuo-Yen Robert Li,(2009).*

a *communication network* as a pair **(G,S)** , where **G** is a finite *directed* multi-graph and **S** is the unique node in **G** without any incoming edges. A directed edge in **G** is called a *channel* in the communication network, (**G, S)**. The special node **S** is called the *source*, while every other node may serve as a *sink* as we shall explain. A channel in graph **G** represents a noiseless communication link on which one unit of information (e.g., a bit) can be transmitted per unit time. The multiplicity of the channels from a node **X** to another node **Y** represents the *capacity* of direct transmission from **X** to **Y**. In other words, every single channel has unit capacity.

At the source **S**, a finite amount of information is generated and multicast to other nodes on the network in the multi-hop fashion where every node can pass on any of its received data to other nodes. At each non source node which serves as a sink, the complete information generated at **S** is recovered. We are naturally interested in how fast each sink node can receive the complete information.

As an example, consider the multicast of two data bits, **B1**and **B2**, from the source **S** in the communication network depicted by Fig. 1(a) to both nodes **Y** and **Z**. One solution is to let the channels, **ST**,**TY, TW**, and **WZ** carry the bit**b1** and channels **SU**,**UZ** and **WY** carry the bit **b2**. Note that in this scheme, an intermediate node sends out a data bit only if it receives the same bit from another node. *Raymond W. Yeung,(2009).*

For example, the node **T** receives**b1** the bit and sends a copy on each of the two channels **TY** and **TW**. Similarly, the node **U** receives the bit**b2** and sends a copy into each of the two channels **UW** and **UZ**. In our model, we assume that there is no processing delay at the intermediate nodes. Unlike a conserved physical commodity, information can be replicated or coded. Introduced in [1] (see also [5, Ch. 11]), the notion of network coding refers to coding at the intermediate nodes when information is multicast in a network. Let us now illustrate network coding by considering the communication network depicted by Fig. 1(b). In this network, we want to multicast two bits**b1** and **b2**from the source **S** to both the nodes and **Z**. A solution is to let the channels **ST** ,**UW** ,**UZ** carry the bit**b2** , channels **WX** ,**XY** ,**YZ** carry the bit , and channels carry the exclusive-OR . Then, the node receives and, from which the bit can be decoded. Similarly, the node can decode the bit from and. The coding/decoding scheme is assumed to have been agreed upon beforehand. It is not difficult to see that the above scheme is the only solution to the problem. In other words, without network coding, it is impossible to multicast two bits per unit time from the source to both the nodes and . This shows the advantage of network coding. In fact, replication of data can be regarded as a special case of network coding.

As we have pointed out, the natures of physical commodities and information are very different. Nevertheless, both of them are governed by certain laws of flow. For the network flow of a physical commodity, we have the following.

The law of commodity flow: The total volume of the outflow from a no source node cannot exceed the total volume of the inflow.

The counterpart for a communication network is as follows. The law of information flow: The content of any information flowing out of a set of no source nodes can be derived from the accumulated information that has flown into the set of nodes.

After all, information replication and coding do not increase the information content. The information rate from the source to a sink can potentially become higher and higher when the permitted class of coding schemes is wider and wider. However, the law of information flow limits this information rate to the max-flow (i.e., the maximum commodity flow) from the source to that particular sink for a very wide class of coding schemes. The details are given in [1]. It has been proved in [1] that the information rate from the source to a set of nodes can reach the minimum of the individual max-flow bounds through coding. In the present paper, we shall prove constructively that by linear coding alone, the rate at which a message reaches each node can achieve the individual max-flow bound. (This result is somewhat stronger than the one in [1]. Please refer to the example in Section III.) More explicitly, we treat a block of data as a vector over a certain base field and allow a node to apply a linear transformation to a vector before passing it on.

A preliminary version of this paper has appeared in the conference proceedings [3]. The remainder of the paper is organized as follows. In Section II, we introduce the basic notions, in particular, the notion of a *linear-code multicast* (LCM). In Section III, we show that with a "generic" LCM, every node can simultaneously receive information from the source at rate equal to its max-flow bound. In Section IV, we describe the physical implementation of an LCM first when the network is acyclic and then when the network is cyclic. In Section V, we present a greedy algorithm for constructing a generic LCM for an acyclic network. The same algorithm can be applied to a cyclic network by expanding the network into an acyclic network. This results in a "time varying" LCM, which, however, requires high complexity in implementation. In Section VI, we introduce the time-invariant LCM (TILCM) and present a heuristic for constructing a generic TILCM. Section VII presents concluding remarks.

5.2.2 Global Encoding Vector

In the year 2011 Jiming Chen, Proposed the idea on Global Encoding Vector in that, Each packet transmitted over the network is a linear combination of the original packets R= {p1,p2,...pn} generated by the source node s. Accordingly for each edge e E we define the global encoding vector , that captures the relation between the packets transmitted on edge e and the original packets in R;

VI. Conclusion

In this paper, an up to date survey on Security analysis in Multi-hop wireless Networks has been presented. The benefits and the issues Caused due to the Network Coding algorithm based Multicast routing has been reviewed. And list the Strengths and weaknesses. Then I have suggested navel network coding and Global Encoding Vector Algorithms to overcome that weakness.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, "Parametric Probabilistic Sensor Network Routing," Proc. ACM Int'l Conf. Wireless Sensor Networks and Applications (WSNA), pp. 122-131, 2003.

[3] M. Burmester and T.V. Le, "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, pp. 405-409, 2004.

[4] T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis, "Securing Wireless Sensor Networks Against Aggregator Compromises," IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141, Apr. 2008.

[5] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, C.E. Perkins, ed., pp. 139-172, Addison-Wesley, 2001.

[6] Y. Wu, P. A. Chou, and S.-Y. Kung,"Minimum-energy multicast immobile ad hoc networks using network coding," IEEE Trans. Commun vol. 53, no. 11, pp. 1906-1918, Nov. 2005.

[7] P. A. Chou and Y. Wu, "Network coding for the Internet and wireless networks," IEEE Signal Process. Mag., vol. 24, no. 5, pp. 77-85, Sep.2007.

[8] Z. Li, B. Li, and L. C. Lau, "On achieving maximum multicast throughput in undirected networks," IEEE Trans. Inf. Theory, vol. 52,no. 6, pp. 2467-2485, June 2006.

[9] E. Ayday, F. Delgosha, and F. Fekri, "Location-aware security services for wireless sensor networks using network coding," in Proc. IEEE INFOCOM '07, pp. 1226-1234, 2007.

[10] M. Wang and B. Li, "Network coding in live peer-to-peer streaming,"IEEE Trans. Multimedia, vol. 9, no. 8, pp. 1554-1567, 2007.