Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature

Yu Zhou¹, Xiaobin Tan², Xianzong He², Guihong Qin² and Hongsheng Xi²

¹Department of Electronic Engineering & Information Science, University of Science and Technology of China, Hefei, Anhui, P.R.China
yzhou86@mail.ustc.edu.cn

²Department of Automation, University of Science and Technology of China, Hefei, Anhui, P.R.China
xbtan@ustc.edu.cn, xzhe@mail.ustc.edu.cn, qingh@mail.ustc.edu.cn, xihs@ustc.edu.cn

Abstract: ExOR is an opportunistic multi-hop routing protocol transmitting packets through multiple routing paths which enhances the throughput of wireless network. Since diverse attacks happen aiming at wireless network routing and ExOR is lack of security, it is necessary to enhance the capability of preventing malicious attack for routing protocol[16][19]. SecExOR, a secure opportunistic multi-hop routing protocol based on ExOR using key-sharing by Lagrange Polynomial Group and digital signature, is proposed in this paper. SecExOR sets up public and private keys to network nodes for authentication before transmitting of packets. Digital signature using unsymmetrical keys and hash function is employed ensuring reality of routing information. Communication keys based on Lagrange Polynomial Group are pre-shared to be used in the encryption of parts of routing information and packet data avoiding leak and disguise. Simulation indicates that SecExOR protocol successfully resists wireless network attacks and displays effective security performance while maintaining the high throughput of original ExOR.

Keywords: ExOR, opportunistic routing, wireless multi-hop network, LPG, digital signature.

1. Introduction
Multi-hop wireless networks, such as ad hoc network and wireless mesh network, typically use traditional routing protocols that are employed in wired networks [3, 15, 14, 12, 13]. The routing techniques used in wired networks choose the best sequence of nodes between the source and destination. Then, packets are sent through this definitive path [3, 4]. Opportunistic techniques using multi-path for routing have been proposed by the information theory community [18, 19], suggesting that definitive path may not be the best approach. Opportunistic routing protocols like ExOR broadcast packets through multiple paths so that transmission capability of signal channels could make the best use. Opportunistic technique is based on simultaneous, synchronized repeating of the radio signal [17] or additional radio channels.

ExOR makes use of multiple paths to forward packets enhancing performance of networks. Nowadays security problems become essential in wireless networks and then attacks and vulnerability cannot be avoided in ExOR. Network attacks aiming at routing protocols influence ExOR as well.

2. ExOR Routing Protocol

2.1 Introduction to ExOR
ExOR is an opportunistic multi-hop routing protocol transmitting packets through multiple routing paths. As an integrated routing and MAC techniques, ExOR aims at enhancing network throughput of multi-hop wireless networks. ExOR realizes part of gains of cooperative diversity on standard MAC protocol such as 802.11.

In ExOR, unlike traditional routing, only one node transmits signals at a time in way of broadcast. Reducing the communication cost of agreement, ExOR operates packets in form of “batch”. After packets are received from upper layer by routing module of source node, they are grouped to batch
by number of a certain batch size. Packets belonging to the same batch are sent by sequence from source node, broadcast to other nodes those are closed to source. Each packet carries a forwarder list indicating forwarders’ priority. Forwarder list is calculated and decided by source node before the transmitting of packets. Link-level measurements in [11] have shown that delivery probability is hard to predict by signal to noise ratio or distance measurements. Forwarder list arranges the forwarding priority of each forwarder by calculating ETX values based on link delivery probabilities to destination node. Fig1 is an example network of five nodes with link delivery probabilities marked on edge of graph.

Figure 1. Example network with link delivery probabilities

Nodes buffer successfully received packets until end of batch. Since the forwarder priority of each node has been decided before transmitting, forwarder nodes will broadcast packets received by sequence set beforehand. Forwarder with higher priority broadcasts its buffered packets earlier so that lower priority node will notice which packets to be sent to high-priority node. Only one forwarder broadcasts packets at a time and forwards transmits signals by sequence defined in forwarder list from source node so that the node closer to destination will transmit earlier. This forwarding sequence is controlled by clocks of each node. Clocking mechanism is one of the key components of ExOR.

Packets are sent with data structure named “batch map” indicating the highest node each packets have reached. Batch map is a list of node address which records the highest priority node where this corresponding packet of the batch has been successfully received. When a forwarder node received a packet, it checks the batch map of packet with its own batch map buffer. If new batch map is later at time than buffer, node updates its batch map buffer and takes out packets that are not received by other nodes with higher priority form its packets buffer. These packets are broadcast so that higher priority nodes could receive them and update their buffer. This procedure goes on and thus the packets buffer of destination node increases continuously. Fig 2 shows the packet header of ExOR.

Figure 2. Packet header of ExOR

2.2 Vulnerability of ExOR

Via the development of secure routing protocols, significant work has been did to ensure the security of ad hoc networks and other wireless networks. As a critical component of secure architecture, resilience to misbehavior and DoS attacks has becoming the focus of research. Diverse network attacks aiming at routing protocols exist and are also influencing ExOR.

Data inconsistency failures caused by malicious nodes are designated as malicious packet modifying attacks (MPA). In ExOR, malicious nodes could participate in transmitting. These nodes may modify the batch map of packets received from other nodes and forward these modified packets and then the performance and throughput of wireless networks will be influenced. [6] To solve this problem, it is necessary to make digital signature for node-decided information included in the header of ExOR packets such as batch map and forwarder list.

Another important situation is that, one malicious node may pretend to be other normal node originally included in the forwarder list. The packets from this imitated node will interfere normal ExOR routing. It is suggested that authentication mechanism should be brought into ExOR so that nodes can authenticate each other before transmitting to avoid participation of malicious nodes.

Besides disguise and interpolation, black-hole attack and gray-hole attack may also happen in ExOR networks. Black-hole attack has two properties. First, the node exploits the wireless network routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Gray-hole attack is as same to black-hole and gray-hole node consumes only part of the packets so that security mechanism could hardly discover this malicious behavior.

Once a malicious node successfully takes charge in the
forwarder list, it is able to drop all packets or part of packets it received. For the sake of these attacks as well as wormhole attack make, capability of the whole networks transmitting packets will fall down[7], [8]. The fatal cause for the occurrence of this type of attack is exactly the lack of authentication mechanism. Avoiding the participation of malicious nodes is more feasible than detecting attacking nodes while routing.

As a conclusion, it is necessary to setup key-sharing and authentication techniques as well as digital signature mechanism in secure architecture based on ExOR to avoid attacks that are of frequent occurrence and more serious everyday.

3. Secure Architecture for ExOR Based on Lagrange Polynomial Group and Digital Signature

The secure architecture for ExOR proposed by this paper includes two main components: Lagrange Polynomial Group (LPG) and digital signature using hash function. LPG is used to share communication keys among authenticated nodes of network so that some parts of packets can be encrypted to prevent being leak. Digital signature using hash function is employed to authenticate the packets from forwarders ensuring the authenticity and integrity of data and batch maps. Before the process of key-sharing for communicating and digital signature for authentication, public keys and private keys should be pre-setup to network nodes.[10]

3.1 Basic idea

Lagrange interpolation polynomial can be used to reconstruct a polynomial from certain numbers of so-called shadow calculated by this polynomial. [9] Assume the order of this polynomial is n, only when more than n-1 shadows are gathered and then the original polynomial can be reined from those shadows. If the communication key is set as the constant term of polynomial, every node could obtain an unique shadow. Due to the characteristic of Lagrange form of interpolation polynomial, only if number of nodes is more than some threshold value, then these nodes could reconstruct the polynomial and calculate the constant term which is the communication key. After that, the transmitting of packets starts out.

In some secure communication protocols for wireless networks, a pair of nodes needs to negotiate a temporary communication key for transmitting encrypted packets. This method needs large number of keys and also increase communication overhead, and thus the throughput of network is influenced. Lagrange interpolation polynomial allows certain number of nodes to share a key together while little number of malicious nodes could not reform the key since the threshold of Lagrange polynomial. A series of Lagrange polynomials call Lagrange polynomials group can be made used to reline different keys as need as possible and this mechanism take much less cost than creating temporary keys between node pairs.

In order to prevent the network form being intruded by malicious nodes, authentication mechanism using unsymmetrical keys should be brought into our SecExOR so that malicious nodes could not take part in the key-rebuild procedure.

3.2 Pre-setup of unsymmetrical keys

As it is noticed in ExOR, nodes which participate in packets transmission are foreknowledge to source node so that it can decide the forwarder list. It is feasible to pre-setup keys to each node ensuring the employment of unsymmetrical keys by authentication and digital signature techniques involved in SecExOR. For one node, a node ID and a pair of public and private key are needed. Every node knows the node ID and public keys of other nodes. Public and private key are generated by key-setup techniques and it is assumed that all nodes being able to take charge in wireless communication have buffered node IDs, private key and public key group before the launch of routing protocol. Unsymmetrical keys can make use of RSA or ECC cryptography system and this paper mainly focuses on authentication techniques but not particular process of keys generation or distribution.

3.3 Digital signature based on pre-setup keys and hash function

In ExOR, forwarders broadcast packets including BatchID, PktNum, BatchSz, FwdListSize and ForwarderList. These five parts are generated by source node thus should not be modified, or else, malicious node could change these information in order to influence the efficiency of ExOR routing technique. In SecExOR proposed by this paper, the five parts noticed above and an appended polynomial ID (will be introduced later) become an entirety named “source-info area” indicating the batch and forwarded information. Source node calculates the signature of “source-info area” and adds it to the header of packets. Forwarder inspects and verifies the signature to make sure “source-info area” is really from source node. Any bad packets with false signature will be dropped.

Fig 3 shows the packet header format. “Forwarder List” field includes source and destination node and other forwarders. “Batch ID” indicates id of batch; “PktNum” indicates sequence number of packet in batch; “BatchSz” indicates number of packets in batch; “FwdListSize” indicates number of forwarders in the forwarder list; “FragNum” indicates sequence number of packet; “FragSz” indicates number of packets in batch the forwarder has received; “ForwarderNum” indicates offset of forwarder in the forwarder list.

Define SIA as “source-info area” which includes the gray fields as in Fig 2, SIG as signature, Encrypt and Decrypt stand for the encryption function of unsymmetrical keys, hash is MD5 or SHA-1 function, SRK is private key and SPK is public key of source node. Source node Calculates “source-info area” signature as in (1). Other nodes check the
signature as in (2).

\[
SIG = Encrypt(hash(SIA), SRK) \quad (1)
\]

\[
hash(SIA) = Decrypt(SIG, SPK) \quad (2)
\]

Since there are additional fields appended to the packet header, size of packet increases. Size of packets decides the entire data size delivering in the network and our appended field will raise network load and effect network performance and throughput. However, the cost due to additional packet header fields is much less than decline of routing efficiency for the sake of malicious attack. The simulation discussed in section 4 confirms this fact.

3.4 Communication keys pre-sharing technique based on Lagrange Polynomial Group (LPG)

In particular situation, it is necessary and essential to encrypt part of data in the packet header to avoid being eavesdropped by irrelevant or malicious node. In ExOR, forwarder list is important information as all nodes participating in wireless communication are involved. Once malicious node understands which nodes are in forwarder list, it can easily fake batch map and forwarder number and so on to interfere the normal routing procedure, thus the whole throughput of wireless network will be affected. And more, when a batch of packets has already arrived destination node, ExOR provides no confirm technique and it is believed not reasonable. In SecExOR proposed by this paper, destination should send ACK packets to source node since a batch of packets successfully received. This ACK packets as well as forwarder list included in normal packets are required to be encrypted by some pre-shared communication keys.

If every node encrypts data using its own private key, other nodes receiving packets broadcasted by this node are able to decrypt data employing its public key. However, the overhead for unsymmetrical keys calculation is much huger on contrary to using usual symmetrical keys. Considering the characteristic of ExOR, packets are broadcasted through multiple path and most nodes take charge in transmitting, a particular key-sharing based on LPG is proposed in this secure architecture.

Before the launch of ExOR routing, a Lagrange Polynomial Group is generated, including a group of Lagrange Polynomials as in (3).

\[
h(x) = (a_{t-1}x^{t-1} + \ldots + a_1x + K) \mod p \quad (3)
\]

\(p\) is a prime number, \(K\) is the communication key to be shared. \(a_1\ldots at-1\) is coefficients of the polynomial. \(t\) decides the degree of the polynomial. Since \(K\) and \(a_1\ldots at-1\) can be other value to form other polynomials, several keys can be shared among groups of nodes.

\[
k_i = h(x_i), i = 1..n, n \geq t \quad (4)
\]

For node \(i\), an integer \(x_i\) is selected and \(h(x_i)\) is calculated to be \(k_i\) as in (4). This pair of integer \((x_i, k_i)\) called “shadow” is pre-setup to node \(i\). After the routing has begun, if one node wants to use the pre-shared keys, it broadcasts special packet with its signature to request shadows of other nodes. Once shadows of at least \(t\) nodes are received successfully, the requesting node is able to recover the communication key as in (5) and (6). Then the recovered key can be used for encryption.

\[
h(x) = \sum_{s=1}^{t} k_i \prod_{j=1, j \neq s}^{t} (x - x_j) \mod p \quad (5)
\]

\[
K = h(0) \quad (6)
\]

Sharing keys among group of nodes can make sure that a very few malicious have no capability to obtain keys because their requesting packets involving wrong signature will be neglected. Lagrange Polynomial Group is used in this schema and source node chooses a particular Lagrange polynomial to recover certain key among the many keys defined in Lagrange Polynomial Group. For different batch, source node can choose different key to obtain better security. In the packet header an area named “polynomial ID” is appended so that forwarders are aware of which polynomial to be used in recovering key. As a result, even though one of the key is leaked, node can choose other keys in stead of changing the entire Lagrange Polynomial Group.

4. Simulation and Performance Analysis

4.1 Simulation environment

Two groups of simulations comparing normal ExOR protocols and SecExOR are implemented using ns2 (the network simulator 2). A 200x100 simulation network with 5 nodes included in the ExOR forwarder list makes up the experimental environment. First group imitates the gray-hole attack and black-hole attack and second group imitates interpolation of batch map. Both groups compare normal ExOR routing, ExOR under attack and SecExOR resisting attack. Fig 4 describes the simulation network graph.

We ran the ns2 simulator five times for each group with
different total packets numbers. The entire time (unit: second) cost to delivery all packets from source to destination is employed to evaluate the performance of every situation.

Figure 4. simulation network graph

4.2 Simulation for interpolation
In the first group of simulation, a malicious node included in the forwarder list falsifies batch map and forwards packets with false batch map to other nodes. This malicious behavior immediately causes the failure of entire network routing of original ExOR. The simulation result indicates segment fault meaning that routing procedure is interrupted by false routing information. While in SecExOR, nodes can authenticate the packet header information using signature to discover packets with false batch map and drop them, preventing malicious nodes of oversetting routing procedure. Simulation results indicate that SecExOR successfully detects malicious behavior and prevents damage with a little more cost than ExOR under no attack. Table 1 and Fig 5 show the simulation results.

4.3 Simulation for gray-hole and black-hole attack
In the second group simulations, there are three schemas to be compared. Normal schema stands for ExOR under no attack. Attack schema stands for ExOR under gray-hole attack and black-hole attack. Secure schema stands for SecExOR under attack. In the attack schema, a malicious node playing gray-hole attack randomly selects some partition of packets received and drops them while malicious node playing black-hole attack drops all packets it received. In the simulation this malicious node is not in the original network and it pretends to be an authenticated node to join in the forwarder list. In ExOR the malicious node successfully participates in the delivering of packets because there is no security mechanism in ExOR. But in SecExOR, malicious node is detected and dropped avoiding influence towards network transmitting. From the result of simulation, it can be concluded that gray-hole attack and black-hole attack influences the performance of ExOR protocols to a large extent. SecExOR can avoid the network from being influenced by malicious nodes while the security mechanism costs little comparing with original ExOR under attack. Table 2 and Fig 6 show the simulation results of second group. Since the SecExOR under attacks takes almost the same time with normal ExOR under no attacks, the two lines of normal and secure schema in Fig 6 seem overlap.

Table 1. Simulation result of first group.

<table>
<thead>
<tr>
<th>Packets</th>
<th>Normal</th>
<th>Secure</th>
<th>Interpolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>49.40s</td>
<td>51.08s</td>
<td>Routing fail</td>
</tr>
<tr>
<td>400</td>
<td>81.10s</td>
<td>87.64s</td>
<td>Routing fail</td>
</tr>
<tr>
<td>600</td>
<td>121.08s</td>
<td>127.72s</td>
<td>Routing fail</td>
</tr>
<tr>
<td>800</td>
<td>151.64s</td>
<td>174.12s</td>
<td>Routing fail</td>
</tr>
<tr>
<td>1000</td>
<td>197.42s</td>
<td>222.34s</td>
<td>Routing fail</td>
</tr>
</tbody>
</table>

Table 2. Simulation result of second group.

<table>
<thead>
<tr>
<th>Packets</th>
<th>Normal</th>
<th>Secure</th>
<th>Gray-hole</th>
<th>Black-hole</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>49.40s</td>
<td>49.53s</td>
<td>71.84s</td>
<td>&gt;5000s</td>
</tr>
<tr>
<td>400</td>
<td>81.10s</td>
<td>81.35s</td>
<td>148.52s</td>
<td>&gt;5000s</td>
</tr>
<tr>
<td>600</td>
<td>121.08s</td>
<td>121.44s</td>
<td>207.73s</td>
<td>&gt;5000s</td>
</tr>
<tr>
<td>800</td>
<td>151.64s</td>
<td>152.12s</td>
<td>260.34s</td>
<td>&gt;5000s</td>
</tr>
<tr>
<td>1000</td>
<td>197.42s</td>
<td>198.04s</td>
<td>332.38s</td>
<td>&gt;5000s</td>
</tr>
</tbody>
</table>

Figure 5. Time cost in first group

Figure 6. Time cost in second group

5. Conclusion and Future Work
In this paper, a secure architecture for ExOR based on
key-sharing by Lagrange Polynomial Group and digital signature is proposed to enhance security performance and routing attack resistance of ExOR. Simulation result indicates that SecExOR has a better efficiency against network attack than original ExOR.

Simulation shows that though SecExOR can detect attack and drop wrong packets from malicious nodes, the performance of network is worse than ExOR under normal situation. The future work may be enhancing forwarding efficiency of SecExOR under routing attack and further completing the technique of SecExOR.

Acknowledgement

Supported by the Knowledge Innovation Program of the Chinese Academy of Sciences, Grant No.YYYYJ-1013

References


Author Biographies

Yu Zhou was born in Hanzhong city of Shaanxi province in 1986. He received the B.S. degree from the University of Science and Technology of China(USTC), Hefei, China, in 2008, and he is studying for a M.S. degree in University of Science and Technology of China (USTC) in Hefei, China. His research field is computer and network security.

Xiao-Bin Tan was born in Xi’an city of Shaanxi province in 1973. He received the B.S. and Ph.D. degrees from the University of Science and Technology of China(USTC), Hefei, China, in 1996 and 2003 respectively. Now, he is working as an associate professor in department of Automation of University of Technology of China (USTC) in Hefei, China and his research field is wireless network security.