584 -Wireless Technical Paper 1

Secure Data Communications in Wireless Networks Using Multi-Path Avoidance Routing

Rahul Godugupally

CWID-10470581

1. Summary of fundamental ideas presented in the paper

In this paper, the authors propose an avoidance routing framework for secure data communication. The framework is named “Timer-based multi-path avoidance routing (TMPAR).” The proposed framework can securely deliver a message m from the source to the destination even in the presence of eavesdropping.

The authors claim that their framework can overcome the problem that arises due to a single path-based protocol as it is “relies on the availability of a safe path, i.e., no adversary is in the proximity of the whole path, which is difficult to achieve and therefore limits the routing opportunity.” [1]

They argue that due to improper software implementation and misuse of cryptography, data encryption can no longer be considered an adequate safeguard against security attacks. For instance, if an attacker with enough time and resources can get a hold of encrypted data, they can decrypt it. To tackle this, they propose a framework which is called multi-path avoidance routing (MPAR) that divides the message into k distinct parts and sends the distinct parts along various paths. The framework also incorporates XOR coding at the destination to get the original message back at the destination.

Further, they combine this technology with timer-based k-path discovery protocol “that identifies a better set of safe paths and reduces the message overhead compared with the original MPAR.” [1] This combined protocol is named TMPAR.

Finally, the authors conduct simulations using ns-2 to evaluate the protocol and show that the protocol significantly improves performance for delivering a message between source and destination compared to existing solutions.

2. Issues paper addresses and how they have been addressed in the past

The key issues that the paper pertains to is data privacy, particularly to prevent unauthorized or malicious users from obtaining or accessing encrypted data which is sent over a network. The authors maintain that due to software implementation failure and misuse of cryptography, data (encrypted data) can no longer be considered safe from attacks. For example, they mention that “approximately 30% of 8,307 public-key certificates of SSL servers randomly chosen from the Internet are vulnerable to the prime number factorization attack due to implementation failure in generating prime numbers [3]”. As more powerful hardware becomes inexpensive and commonplace, they argue that the encrypted data can be decrypted within a sufficient amount of time without having the encryption key. Any cryptographic protocol can be decrypted if time is not a concern, as we see data being decrypted with either brute-forcing or with cracking software which takes the help of powerful GPUs to decrypt the data much faster compared to a few years ago where the computational power was limited.

Furthermore, they state that nation-states with unlimited resources could compromise the communications of another nation by eavesdropping and this renders the communications insecure. They mention the example of “successful cryptanalysis of the Enigma machines by the British Intelligence,”[1] which became a major factor in the Axis’s defeat to the Allies in World War II in which Alan turing had a important part to play.

To prevent data from being accessed by unauthorized party's various path avoidance routing protocols have been proposed in the past, in these routing protocols, insecure nodes are avoided, such that the path does not contain any adversary.

These solutions were designed for Border Gateway protocol (BGP) or distance-vector networks. However, these approaches assume that there is a safe path between source and destination in which there is no node on which adversary can eavesdrop. The authors argue that this is a very rare situation “especially when the wireless ad hoc network is considered where the number of possible paths between source and destination is often very limited due to fluctuated nodal density, power-saving topology control or other reasons.” [1]

3. Discussion of core ideas of the paper

The authors propose an avoidance routing protocol for ad hoc networks by adding to their work already done in [2]. The core idea of their proposed scheme is a combination of multi-path routing and the XOR coding in which a message m is divided into k different parts namely m1, m2,…..mk at the source node. The original message m is obtained back at the destination node by doing XOR operation on all the message parts i.e., $m = m1 \oplus m2 \oplus ...\oplus mk$. Here, $\oplus$ is XOR operation.

Based on the Multi path routing protocol the source node selects paths p1,p2,....pk and sends each different part of the message I.e., m1, m2.....mk via each path. By doing this an adversary cannot decipher the message sent by obtaining a single part of the message. For the adversary to obtain an entire message they would need to have obtained all the k parts of the message which is exceedingly difficult to achieve.

They claim that overhead only increases in networks where distance vector avoidance protocols do not work. And that it yields the same overhead in networks where existing multipath protocols are supported.

They further improve upon the proposed framework by incorporating it with timer-based k-path route discovery protocol. The k-path discovery protocol uses a defer time to find a set of paths with fewer adversaries and optimizes the protocol by avoiding unnecessary route discovery which in turn leads to reduced overhead.

In this protocol the source node sends route requests all over the network then the destination node sends the list of adversaries it may have encountered. After the first iteration, the source node floods the route request a second time to the paths which contain adversaries as reported by the destination node. This process is repeated until the adversary disjoint paths are found on the network or the number of iterations exceeds k (I.e. the number of parts in which the message is divided). This is done to discover a safe path between source and destination if they exist. This phase is known as the route discovery phase.

At every forwarding process at each node, the node starts a timer. With this timer, they can determine the nodes with fewer adversaries as they are faster to deliver the message compared to nodes with more adversaries connected to them. Hence there is more probability of nodes with fewer adversaries being selected on each iteration of the route discovery process. Due to this, the TMPAR requires fewer adversary disjoint paths than the MPAR. Hence it results in lower message transmission cost and control overhead.

Based on the result of the route discovery phase the source node sends the message m via various paths discovered which do not contain adversaries. It could be in a single path mode, k-path mode or it can refrain from sending the message m if it does not find a safe path. Thus, the source node discards m in the last case.

Finally, the given two protocols (MPAR and TMPAR) are compared with an ideal protocol and greedy-AA protocol in their ns-2 implementation. They are compared on various metrics such as delivery rate, end-to-end delay, control overhead, delivery rate under collusion attacks, adversary detection rate etc. In the results, they observe that the proposed protocols perform significantly better than the greedy-AA protocol and remain close to the ideal protocol performance on almost all of the considered metrics.

4. Identification of any security-related issues brought up in the paper

The two major security related issues they address are:

Eavesdropping: if an adversary A is a neighbor of a node, then he can eavesdrop on the transmitted data and break the encryption in a reasonable amount of time unless encryption is of perfect secrecy. This implies that a routing path should avoid insecure areas, or equivalently, nodes that have an adversary in their neighborhood.

Additionally, an encryption scheme of perfect secrecy can prevent eavesdropping as this would mean an attacker with unlimited computational power is not able to get the original message with high probability. But it would not be able to secure against the next security issue.

Denial of service: if any one node of k paths contains an adversary, then they can deny forwarding the data which makes it so that the data cannot be assembled back at the destination node and can also obtain the content of the message (by decryption).

This means that a routing path should never contain an adversary as an intermediate node. Even if the data achieves perfect secrecy, it would still be useless in case of denial of service as one or more of the message parts do not reach the destination node. Hence the data cannot be put back together at the destination.

Here the adversaries are assumed to have unlimited computational power and resources. They claim that avoiding insecure areas is the primary countermeasure. As the first step for hackers is eavesdropping or blocking traffic.

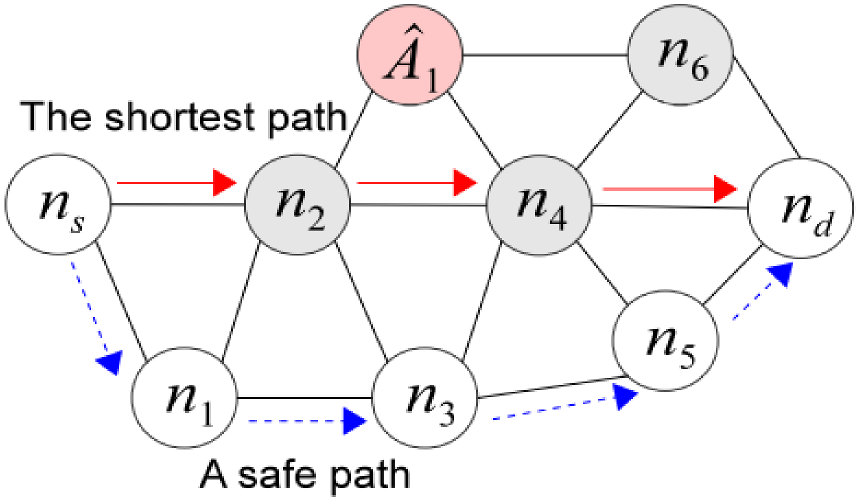

Figure 1 [1]

Here in figure 1, we observe that the path n1, n2, n4, nd is the shortest path but it is avoided as it contains an adversary node(A1) connected to nodes n2, n4 which could lead to eavesdropping. The selected path (safe path) is free of any adversary in its proximity, hence that is chosen.

5.Potential applications of technology presented

The authors believe that their framework will serve as a foundation for critical communications where the attackers have enough time and resources to decipher the encrypted data.

The technology proposed in the paper can indeed be used in various fields where privacy and confidentiality are of primary concern and an adversary could have infinite resources. For example, it can be used for military communications where it is imperative that the data being transmitted does not fall into the wrong hands.

Also, it can be used for secure end to end communications for critical data for everyday use. This could be anything from financial transactions, secure data transfer to the cloud etc. The protocol is extremely beneficial for ad hoc networks where there is no defined set of nodes or access points for data communication over a network.

Further the technology presented in the paper could be used to build a source to destination path scanner that detects adversaries or insecure nodes in each path. That could in turn help in identifying which path is safe for us to send data through along with identifying the malicious nodes in each path which can then be dealt with.

6.Future opportunities created by the technology

The technology proposed in the paper can be further improved in real world scenario, where the "adversary's locations are unknown, by selecting a set of physically distanced paths." [1] Hence it can lead to more opportunities in research.

The technology presented can help in sending messages through an insecure set of paths where adversaries are strategically placed. With the help of avoidance routing and XOR encoding this can be achieved with high success rate.

This could indeed help in improving the state of ad hoc networks by overcoming issues faced by ad hoc networks compared to traditional networks such as reliability, efficiency, and security. This could help to see ad hoc networks slowly start replacing traditional networks.

-Citations

[1] K. Sakai, M. Sun, W. Ku, J. Wu and T. H. Lai, "Secure Data Communications in Wireless Networks Using Multi-Path Avoidance Routing," in IEEE Transactions on Wireless Communications, vol. 18, no. 10, pp. 4753-4767, Oct. 2019, doi: 10.1109/TWC.2019.2928801.

[2] K. Sakai, M. Sun, W. Ku, J. Wu and T. H. Lai, "Multi-path Based Avoidance Routing in Wireless Networks," *2015 IEEE 35th International Conference on Distributed Computing Systems*, 2015, pp. 706-715, doi: 10.1109/ICDCS.2015.77.

[3] R. Nojima, T. Kurokawa, and S. Moriai, “XPIA, X.509 certificate public key investigation and analysis system,” NICT News, vol. 435, pp. 5–6, Dec. 2013.