International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 6 June 2015

Substitute Between Reliability and Safety Measures In Multiple Access Relay Networks Under Inaccurate Data Injection Attack

Mrs.N.B.Divya[1], Mr.P.Hariharan[2]
Research Scholar, Departmentof computer Science, Adhiparasakthi College of Arts & Science, G.B.Nagar,Kalavai, Vellore District, Tamilnadu, India[1]
Assistant Professor, Departmentof computer Science, Adhiparasakthi College of Arts & Science, G.B.Nagar,Kalavai, Vellore District, Tamilnadu, India[2]
nbsowmi@gmail.com[1], plr_hari@rediffmail.com[2]

Abstract: *We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays, which may inject falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node. In addition, parity bits are added to correct the errors caused by fading and noise. When the total amount of redundancy, tracing bits plus parity bits, is fixed, an increase in parity bits to increase the reliability requires a decrease in tracing bits, which leads to a less accurate detection of malicious behavior of relays, and vice versa. We investigate the tradeoff between the tracing bits and the parity bits in minimizing the probability of decoding error and maximizing the throughput in multisource, multi relay networks under falsified data injection attacks. The energy and throughput gains provided by the optimal allocation of redundancy and the tradeoff between reliability and security are analyzed.*

Keywords: *WSN, Multipath Relay, Anonymous Route Discovery, False Data Injection Attack Detection,SNR.*

1. INTRODUCTION

In hybrid ad hoc wireless network, the mobile nodes usually act as routers to relay others' traffics for enhancing the network performance and deployment. Multi-hop packet relay extends the base stations' coverage area without additional cost. It also enhances the network throughput and capacity due to reducing the transmission interference area by transmitting the packets over shorter hops. However, the nature of the wireless transmission and multi-hop packet relay makes the network highly vulnerable to serious security challenges.
Although the proper network operation requires the nodes' cooperation in relaying others' packets, the selfish nodes will not cooperate without sufficient incentive to save their resources. This behavior significantly degrades the network connectivity and packet delivery ratio and may result in failure of the multi-hop communication. Moreover, the attackers can analyze the network traffic to learn the users' locations in number of hops and their communication activities causing a severe threat for the users' privacy.

Due to the open environment and the shared wireless medium, an attacker can intercept all the transmissions within the reception range of his radio receiver without the need to physically compromise a node. Moreover, multi- hop packet relay necessitates processing the packets by the mobile nodes to route them. This means that the packets' headers should not be encrypted to enable multi hop routing. Unfortunately, attackers can inspect packets' headers to gain sensitive information. These attacks can be launched in an undetectable way by overhearing transmissions without disrupting the protocol.

Objective:

We propose lightweight protocol for securing communication and preserving users' anonymity and location privacy in hybrid ad hoc networks. Symmetric-key-cryptography operations and payment system are used to secure route discovery and data transmission. To reduce the overhead, the payment can be secured without submitting or processing payment proofs (receipts). To preserve users' anonymity with low overhead, we develop efficient pseudonym generation and trapdoor techniques

that do not use the resource-consuming asymmetric-key cryptography. Pseudonyms do not require large storage area or frequently contacting a central unit for refilling. Our trapdoor technique uses only lightweight hashing operations. This is important because trapdoors may be processed by a large number of nodes.

2. Related work

In this work, we considered a multiple access relay network and investigated the following two problems: Tradeoff between reliability and security under falsified data injection attacks; Mitigation of Forwarding Misbehaviors in Multiple access relay network. In the first problem, we consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays which may inject a falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node.In the second problem, we propose a physical layer approach to detect the relay node that injects false data or adds channel errors into the network encoder in multiple access relay networks. The misbehaving relay is detected. We exploit the detection outcome to enhance the reliability of decoding by erasing (discarding) The data received from the adversarial nodes and correcting the erasuresThe motivation is that erasures can be corrected twice as many as errors. However, the information in the presence of attack may not be perfect in practice. The false alarm results in an erasure of correct bit, while the miss detection may result in an error in place of an erasure. The receiver then computes the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. If the correlation between them is above a threshold then we decide that the relay node is cooperative and, otherwise, it is malicious. The threshold can be chosen to achieve a target false alarm, misdetection, or error probability. The authors of propose a statistical detection technique in order to mitigate malicious behavior in adaptive decode and forward (DF) cooperative diversity. Optimal allocation of redundancy between tracing bits and parity bits that minimizes the probability of decoding error or maximizing the throughput. The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker.

2.1 Disadvantages

- Self certified public key system, certificate verification and management.
- Certificate is replace by a witness and the public key is embedded in it
- Long-term identity or a permanent group of pseudonyms can violate user's privacy.
- Limited number of retransmissions allowed per packet, packet sizes and the impact of acknowledgment packets.
- Message and the identities of the nodes in the route and appends the signature to the data packet.

2.2 Pseudonym Generation Technique

The explicit use of a long-term identity or a permanent group of pseudonyms can violate users' privacy. Attackers can link the identity or the pseudonyms to the user, e.g., by analyzing the associated activities. To preserve users' anonymity, each pseudonym is used for short time in such a way that only the intended node can link the pseudonyms to each other. By this way, even if an attacker could link a pseudonym to the user in one occasion, he cannot violate the user's privacy for a long time and will not benefit from this conclusion in the future due to pseudonyms' period ic change and unlikability. Using a pseudonym for a long time enables attackers to collect much information about the visited locations by the anonymous user. Then, by analyzing this information, the attackers may identify the users and gain much information about their past visited locations.

Adversary Model: The mobile nodes are potential attackers because they are autonomous, self-interested, and motivated to misbehave to increase their welfare. The network infrastructure including Tp and the base stations are secure. They are operated by a single operator that is interested to ensure the network security. The adversaries can be legitimate nodes which have valid keys to access the net- work, or external adversaries who are not members in the net- work. They may also work individually or collude with each other to launch sophisticated attacks.

2.3 Anonymous Route Discovery

Uplink Route Request Packet (URREQ): The source node initiates route discovery by broadcasting URREQ packet containing a unique request identifier (Uni), time to live (TTL), and the encryption of Uni, the source and the destination nodes' real identities, dummy bits called padding (Pad), and the padding length (PL). Uni is the pseudonym shared with Bs (IDSBs) and time stamp. Each node and the base station process only the first received URREQ packet

Destination Notification Packet (DNOT): The destination base station (Bd) receives a call request for a

node in its cell; it notifies the node by broadcasting Destination Notification Packet (DNOT). The packet contains a unique identifier (Dni) that has the pseudonym shared with D and time stamp. The packet also contains Time-to-Live (TTL), and the encryption of Dni and the destination and source nodes

Downlink Route Request Packet (DRREQ): The destination node composes and broadcasts the DRREQ packet. Processing the packet is similar to that of the URREQ packet.

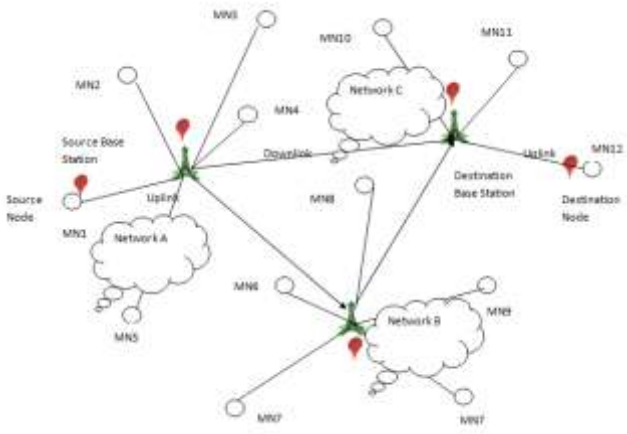

Fig 1.1: System Architecture

Figure 1.1 shows an example of multiple access relay network. In multiple-access relay network (MARN), multiple sources communicate with single estimations in the presence of relay nodes. Examples of such networks include hybrid wireless LAN/WAN networks and sensor and ad hoc networks where cooperation between sources is either undesirable or not possible, but one can use an intermediate relay nodes to aid Communication between the sources and the estination. As in multiuser wireless systems, access coordination among sources may be carried out in different domains: the frequency domain, time domain, code domain, and space domain. Signals of different sources are insulated in each domain by splitting the resource available into non-overlapping slots (frequency slot, time slot, code slot, and space slot) and assigning each signal a slot. Four main multiple access technologies are used by the wireless networks: frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and space division multiple access (SDMA).

3. MULTI RELAY NETWORK

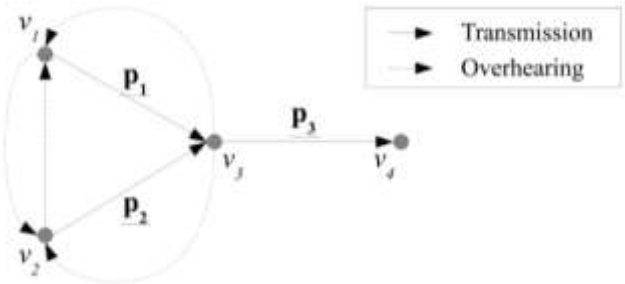

Fig 3.1: E.g- Wireless Senosr Network

A node $vi \in V$ transmits coded information xi by transmitting a packet pi, where $pi = [ai,hIi,hxi,xi]$ is a $\{0, 1\}$-vector. A valid packet pi is defined as below:

- *ai* corresponds to the coding coefficients $\alpha j, j \in Ii$, where $Ii \subset V$ is the set of nodes adjacent to vi in E1
- *hIi* corresponds to the hash $h(xi), vj \in Ii$ *where* $h(.)$ is a h-bit polynomial hash function
- *hxi* corresponds to the hash $h(xi), vj \in Ii$ *where* $h(.)$ is a h-bit polynomial hash function.
- xi is the n-bit representation of $xi = Pj \in I\ \alpha jxj$

The goal is to explore an approach to detect and prevent malicious behaviors in wireless networks using network coding. The scheme takes advantage of the wireless setting, where neighbors can overhear others transmissions albeit with some noise, to verify probabilistically that the next node in the path is behaving given the overhead transmissions.

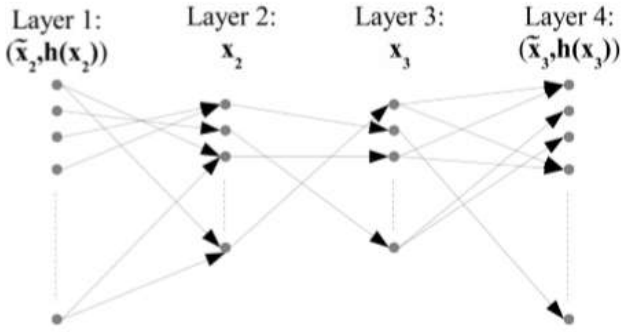

Fig 3.2 A graphical model from v1s perspective.

Authors proposed two models in their paper. The graphical model is used to explain how a node *v1* checks the behavior of its neighbor *v2*. Then, the algebraic approach is used for analysis.

As shown in Figure 3.2, the graphical model has four layers: Layer 1 contains $2n+h$ vertices, each representing a bit-representation of $[e\ x2,h(x2)]$; Layer *2* contains *2n* vertices, each representing a bit-representation of *x2*; Layer *3* contains *2n* vertices corresponding to *x3*; and

Layer 4 contains *2n+h* vertices corresponding to *[e x3,h(x3)]*. Edges exist between adjacent layers as follows:
Layer 1 to Layer 2: An edge exists between a vertex *[v,u]* in Layer 1 and a vertex w in Layer 2 if and only if *h(w) = u.* The edge weight is normalized such that the total weight of edges leaving *[v,u]* is 1, and the weight is proportional to *P(v| Channel statistics and w is the original message)* which is the probability that the inference channel outputs message v given an input message *w*.
Layer 2 to Layer 3: The edges represent a permutation. A vertex *v* in Layer 2 is adjacent to a vertex w in Layer *3* if and only if *w = c+α2v, where c = α1x1* is a constant, *v and w* are the bit-representation of *v and w*, respectively. The edge weights are all 1.
Layer 3 to Layer 4: An edge exists between a vertex v in Layer 3 and a vertex [w,u] in Layer 4 if and only if h(v) = u. The edge weight is normalized such that the total weight leaving v is 1, and is proportional to P(w| Channel statistics and v is the original message)
Node v1 overhears the transmissions from *v2* to *v3* and from *v3* to *v4*; therefore, it receives*[e x2,h(x2)]* and *[e x3,h(x3)]*,
corresponding to the starting point in Layer 1 and the destination point in Layer 4 respectively. By computing the sum of the product of the weights of all possible paths between the starting and the destination points, *v1* computes the probability that *v3* is consistent with the information gathered.

IV. SYSTEM IMPLEMETNATION

4.1 Multiple Access Relay System

A multiple access relay network where multiple sources send independent data to a single destination through multiple relays. Multiple relay systems maintain the current information of the sources connection details and the respective files details. As per request and response relay system communicate with the source systems. In multiple access relay networks, relay nodes may combine the information‘s received from different sources to generate scheduling process as per destination request and forward the request to respective short listed source.

4.2 Source Response

System As per relay node request each source send the periodic update information about its connection status and the files information. The source generates independent packets after get the file request from the relay node then generate source key which is based on the contents in the file like reference/tracing bits. Then classify the destination system form the request packet and route the file to the destination system. At each source, the tracing bits are embedded in the k message bits using a position key κp which is common for all sources and is known to source nodes and the destination The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker.

4.3 Destination Request System

To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node. The destination node then computes the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. Destination system sends the file request to the relay node and waits till the file gets download. After getting download request from the source system, the destination system accept the download request and classify the packet for to identify any false data may injected and identify the malicious relay node.

4.4 False Data Injection Attack Detection

This module exploit the detection outcome to enhance the reliability of decoding by erasing (discarding) the data received from the adversarial nodes and correcting the erasures. Here, the tracing bits are to identify the malicious relay nodes and erase the data received from them. Generate the data references for the content in the received file and calculate the distance between the data and find the similarity than compare with threshold, finally identify the malicious activity of relay node and the injected data.

4.5 Algorithm Implementation

Detection Algorithm

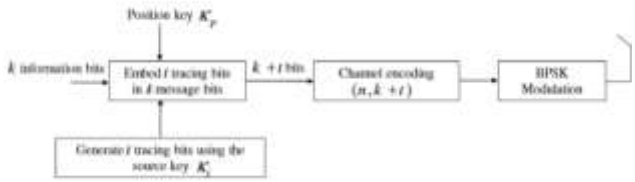

Fig 4.1: Detection Algorithm

Figure 4.1 shows the schematic diagram of detecting malicious relay nodes. The i-th source node uses a secret key *κi* to generate a tracing sequence *Ci = {ci1, ci2, ···, cit}*. We assume that κi is known only to the destination and the *i-th* source node. At each source, the tracing bits are embedded in the k message bits using a position key κp which is common for all If ***d* is greater than a threshold, the destination decides that the relay is malicious, and, otherwise, the relay is cooperative. The first term of *(4.1)* is 2t if alm, flm *∈ {+1, −1}*, and the second term is the cross correlation between Al and Fl. Since the first term of *(4.1)* is constant, the proposed detection algorithm relies only on the correlation co-efficient between *Al and Fl.* The following detection algorithm is applied at the destination to detect malicious relay nodes.**

EVALUATION RESULT

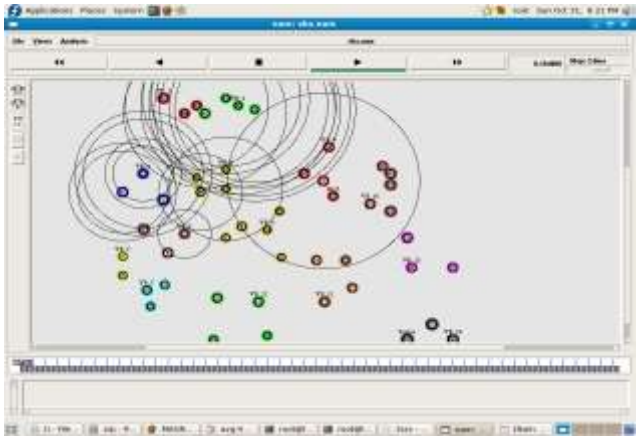

Fig 4.3 Wireless sensor network NAM Create

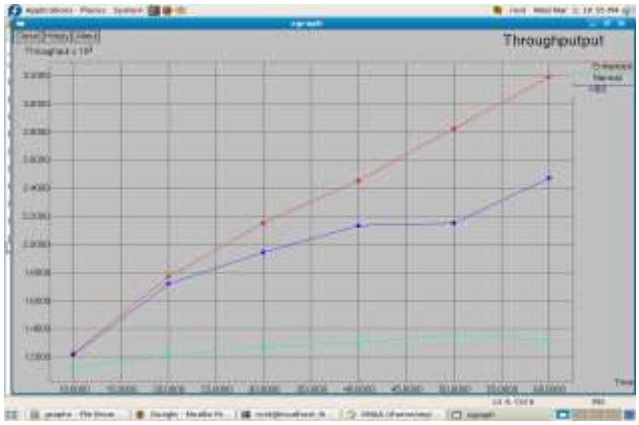

Fig 4.4: Throughput

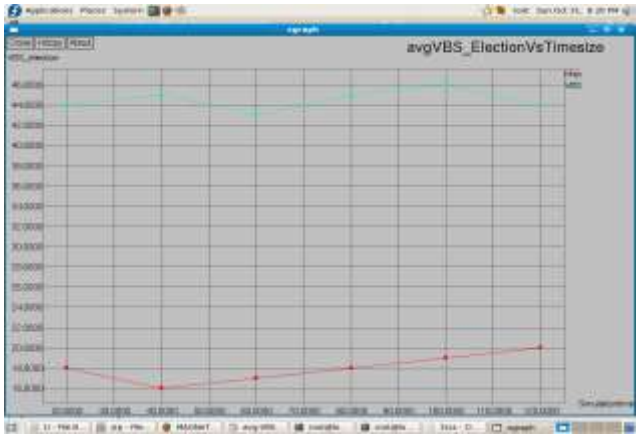

Fig 4.5 Time Size Vs Election Time

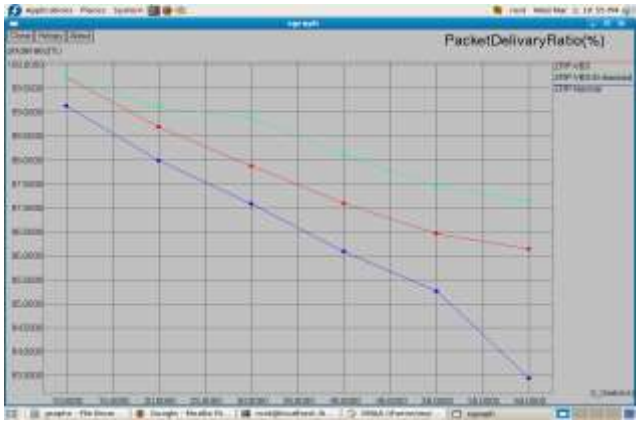

Fig4.6: Packet Delivery Ratio

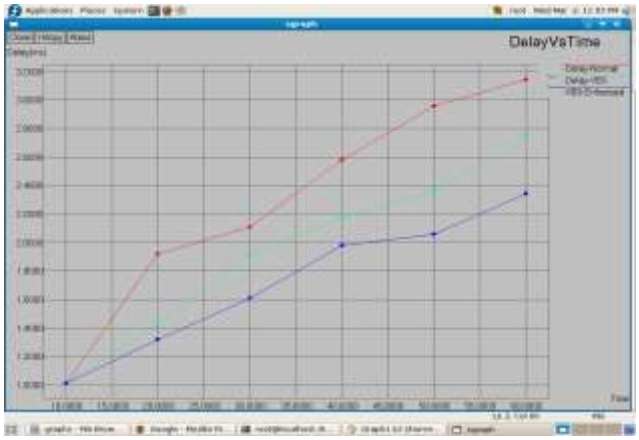

Fig 4.6 Delay Vs Time

CONCLUSION:

We investigated the tradeoff between tracing bits and parity bits, where the former is to identify the malicious relay nodes and discard (erase) the bits received from them and the latter is to correct the errors caused by channel impairments such as fading and noise. We found that there exists an optimal allocation of redundancy between tracing bits and parity bits that minimizes the probability of decoding error or maximizing the throughput. When the total amount of redundancy (sum of tracing bits and parity bits) is fixed, more redundancy should be allocated to the tracing bits for higher probability of being malicious and less on the tracing bits for lower SNR. We analyzed the energy gain (saving) and the throughput gain provided by the optimal redundancy allocation. Future analysis to overcome the drawbacks, enhance the system to achieve more scalability. If any sources update any file location, it needs to update the location information which maintain in the relay system thus overcome the false routing. If any source goes offline i.e. disconnect from the relay systems thus is must indicate offline mode in the relay node if so it must not consider for routing. By implementing these steps as our enhancement with the system, we overcome the drawbacks and get the high scalability as well as certain information about the source mode status and files location

REFERENCES

[1] J. N. Laneman, D. N. C. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[2] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communi- cation in wireless networks," IEEE Commun. Mag., vol. 42, no. 10, pp. 74–80, Oct. 2004.

[3] S. W. Kim, "Cooperative spatial multiplexing in mobile ad hoc net- works," in Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. Conf., Washington, DC, USA, Nov. 2005, pp. 387–395.

[4] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wire- less networks," in Proc. IEEE ISIT, Adelaide, SA, USA, Sep. 2005, pp. 2065–2069.

[5] Y. Chen, S. Kishore, and J. Li, "Wireless diversity through network coding," in Proc. IEEE WCNC, Las Vegas, NV, USA, Apr. 2006, pp. 1681–1686.

[6] X. Bao and J. Li, "Matching code-on-graph with networks-on-graph: Adaptive network coding for wireless relay networks," in Proc. Allerton Conf. Commun., Control Comput., Champaign, IL, USA, Sep. 2005, pp. 1–10.

[7] C. Hausl and P. Dupraz, "Joint network-channel coding for the multiple- access relay channel," in Proc. 3rd Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw., Reston, VA, USA, Sep. 2006, pp. 817–822.

[8] S. W. Kim, S. G. Kim, and B. K. Yi, "Decentralized random parity for- warding in multi-source wireless relay networks," in Proc. IEEE Global Telecommun. Conf., Washington, DC, USA, Nov. 2007, pp. 3937–3941.

[9] F. Zhao, T. Kalkert, M. Medard, and K. J. Han, "Signatures for content distribution with network coding," in Proc. IEEE Int. Symp. Inf. Theory, Nice, France, Jun. 2007, pp. 556–560.