International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 08, August - 2017

Mitigation of Wormhole Attack using Exclusive Algorithms in Manets

Pooja A Patil
PG student Department of CSE
PDA College of engineering, Kalaburagi.

Anuradha T
Department of CSE
PDA College of engineering, Kalaburagi.

***Abstract*—Advancement in wireless technologies and extended the use of wireless devices demand more and more infrastructure less networks like mobile ad hoc networks. As mobile adhoc network applications fan out security emerges as a central requirement. Wireless networks gain higher performance by using network coding .Network coding is a promising generalization of routing, which allows a node to generate output messages by encoding its received messages. However network coding also introduces new attacks such, as well studied pollution attacks and wormhole attack. Wormhole attack, sabotage the performance gain of network coding. Since the characteristics of the network coding system are distinctly different from traditional wireless networks .In wormhole attack malicious node records control traffic at one location and tunnels it to another compromised node, possibly far away, which relays it locally. A centralized algorithm proposed to detect wormholes and show its correctness attendant For the distributed wireless network, DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems is proposed by delving into the change of the flow directions of the innovative packets caused by wormhole. Both the algorithms use node centric information instead of packet centric information, as the underlying network use network coding .Simulation results on NS 2 exhibit the effectiveness of the proposed algorithms in detecting wormhole attacks.**

Keywords—*centralized algorithm, distributed algorithm, expected count of transmission.*

I INTRODUCTION

Network coding is a technique which can be used to improve a network throughput, efficiency and scalability. Future networks are expected to move from traditional routing schemes to network coding based schemes, which have created a lot of interest both in academia and industry in the recent years. Under the network coding paradigm, intermediate nodes store and forward packets as original. In contrast, in wireless network coding systems, the forwarders are allowed to apply encoding schemes on what they receive, and thus they create and transmit new packets. The idea of mixing packets on each node takes good advantages of the opportunity, diversity and the broadcast nature of wireless communications, and significantly enhances system performance[1],[2].This type of communication has proved to be more robust to packet losses, be resilient to network changes such as dynamic topologies, and improve the overall throughput.

To investigate wormhole attacks in wireless network coding systems, we focus on their impact and countermeasures in a class of popular network coding scheme—the random linear network coding (RLNC) system. In this system, in order to best utilize resources, before data transmissions, routing decisions (i.e., how many times of transmissions a forwarder should make for each novel packet) are made based on local link conditions by some test transmissions. Since in wireless network coding systems the routing and packet forwarding procedures are different from those in traditional wireless networks, the first question that we need to answer is: Will wormhole attacks cause serious interruptions to network functions and downgrade system performance? Actually no matter what procedures are used, wormhole attacks severely imperil network coding protocols. In particular, if wormhole attacks are launched in routing, the nodes close to attackers will receive more packets than they should and be considered as having a good capability in help forwarding packets. Thus they will be assigned with more responsibility in packet forwarding than what they can actually provide. Furthermore, other nodes will be correspondingly contributing less. This unfair distribution of workload will result in an inefficient resource utilization and reduce system performance.

Wormhole attacks launched during the data transmission phase can also be very harmful. First, wormhole attacks can be used as the first step towards more sophisticated attacks, such as man-in-the-middle attacks and entropy attacks. For example, by retransmitting the packets from the wormhole links, some victim nodes will have to process much more non-innovative packets that will waste their resources; these constitute entropy attacks. Second, the attackers can periodically turn on and off the wormhole links in data transmissions, confusing the system with fake link condition changes and making it unnecessarily rerun the routing process. To further quantify the impact of wormhole attacks in wireless network coding systems, we perform extensive experiments and investigate the results.

The main objective of this paper is to detect and localize Wormhole attacks in wireless network coding systems. Themajor differences in routing and packet forwarding rule out using existing countermeasures in traditional networks [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]. In network coding systems like

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 08, August - 2017

MORE[5], the connectivity in the network is described using the link loss probability value between each pair of nodes, while traditional networks use connectivity graphs with a binary relation (i.e., connected or not) on the set of nodes. For this reason, prior works based on graph analysis [6], [8], [10], [14] cannot be applied. Some other existing works rely on the packet round trip time difference introduced by wormhole attacks to detect those [13], [15], [16]. Unfortunately, this type of solutions cannot work with network coding. The fundamental reason is that with network coding, the packets being transmitted on each hop are different. They require either to use an established route that does not exist with network coding, or to calculate the delay between every two neighboring nodes which will introduce a huge amount of error in network coding systems.

II.SYSTEM MODEL

In this section we consider the existing system design and the proposed system.

A .Existing System

Existing solutions can be divided into two groups Utilizing temporal ,spatial information and detecting network topology change Hu et al. use packet leashes to detect wormhole attacks, by appending in each packet the location information of the senders and they accordingly detect the physically impossible transmissions. Some of the existing work based on the round-trip travel time of packet to detect wormhole links. Khalil et al. introduced the guard node to help the local node detect the malicious attackers, assuming the network had a static topology. There were two limitations for the methods dependent on time and space: the nodes in the network have to be tightly synchronous and the node location information is available. In the second group, among others, Wang and Bhargava use visualization methods to detect wormhole links in sensor networks, revealing the intrinsic change of network topological structure under attacks. Dong et al. detect and locate various wormholes and relies on observing inevitable topology deviations introduced in the network by wormholes. There is no solution of the wormhole attack detection for wireless network coding systems.

B. Proposed system

A centralized algorithm is proposed to detect wormholes leveraging a central node in the network. For the distributed scenarios, a distributed algorithm is proposed, DAWN, to detect wormhole attacks in wireless intra flow network coding systems. In DAWN, during regular data transmissions, each node records the abnormal arrival of innovative packets and share this information with its neighbors. This algorithm is efficient and practical without strong assumptions. The main idea is that to examine the order of the nodes to receive the innovative packets in the network, and explore its relation with a widely used metric, expected count of transmission (ECT), associated with each node. To propose a centralized algorithm to detect wormholes. In this algorithm, a central node collects the information from all the nodes in the network and analyzes whether there exists a wormhole link. The algorithm leverages the order of the nodes to receive the innovative packet, and utilizes machine learning techniques to distinguish the wormhole cases.

III.DESIGN CONSTRUCTION

In this work, we consider a wireless network with a set of homogeneous nodes running network coding protocols (including routing protocols to calculate the number of per-packet transmissions for each node, and data transmission protocols). Nodes are connected via loss wireless links. For any two nodes u and v in the network such that the successful transmission rate between u and v, p (u, v)> 0, then we say u and v are neighbors. We assume that ECTs are calculated to describe the network topology and are measured periodically to support routing functions. Each node knows its own ECTs and its neighbors' ECTs.

In the wireless network systems, we consider that public key infrastructure (PKI) is in place to implement the public key cryptographic techniques. For the wireless network, we regard each node[1] as a user who has a pair of public and private keys. The identity and the public key of each use rare managed by the certificate authority (CA), which is a trusted entity. If any node A wants to safely communicate with node B, A has to request B's public key from the CA first. After the transmission, node B has to request A's public key from the CA in order to verify the message from A.CA is also responsible to per-distribute and revoke the key pairs of the nodes. The nodes and the CA together form the PKI, which can guarantee that no node can forge reports from other node.

In wormhole attacks, the attackers between distant locations transmit packets using a out-of-band tunnel. The transmission tunnel is called a wormhole link. The packet loss rate on the wormhole link is negligible. The kinds of the wormhole links can be various, such as an Ethernet cable, an optical link, or a secured long-range wireless transmission. When the wormhole attack is initiated, the attackers can capture data packets on either side, forward them through the wormhole link and rebroadcast them on the other node. Here each node includes the normal nodes in the wireless network and the central administrator, which presents in our centralized algorithm.

Linear network coding (LNC), especially random linear network coding. Linear network coding permits each node in the network to pass on the combinations of the received data, in order to optimize the information capacity. Let $r_1, r_2, , , r_n$ denote the received data, and s be the encoded data to be passed to another node. We can obtain the combination f based on the received data based on Equation (1).

$$S = f(r_1, r_2 \ldots r_n) \quad (1)$$

For RLNC, f in Equation (1) is a random linear combination in the field GF (2^k).

$$f(r_1, r_2, \ldots, r_n) = \sum_{i=1}^{n} \varepsilon_i r_i \quad (2)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 08, August - 2017

Here, ε_i is a randomly generated coefficient. In network coding, every node except the recipient applies a random linear mapping from the inputs to outputs over the field GF(2^k). Each packet contains a vector in them-dimensional code vector space V particularly, each packet sent by the source node contains a basis of the code vector space V. If one intermediate node receives a packet which is linearly independent from previous packets, this packet is called an innovative packet. Essentially, an innovative packet must contain at least one basis that the node has not received, and the arrival of an innovative packet will increase the rank of the received packets by one. When the destination receives m innovative packets, whose vectors are linearly independent from each other, it can restore the source information S based on the received data R:

$$S = C^{-1}R \quad (3)$$

Here C is the matrix of the coefficients of the received packets. Since each received packet is essentially a linear combination of the original packets from the source, we can perfectly restore the original messages by multiplying the inverse of C. The capacity of RLNC converges to the optimum in probability, and owns an ideal performance on the compression of the transmitted data. However, since the packet can derive various forms during the transmissions in network coding, when the wormhole attack is initiated, it is difficult to apply some traditional solutions (i.e., tracing the time stamps of a particular packet) to defend. Thus, the wide applications of network coding push us to find another way to defend against wormhole attack.

A.THE CENTRALIZED ALGORITHM

We propose the centralized algorithm, which utilizes the ECT metric and the order of rank increment to detect wormhole attacks. In order to protect the validity of our method, we also introduce the public cryptographic scheme for the network. For each forwarding node in RLNC network, receiving the innovative packet will cause the rank of the previously received packets increases by one. We also find that the nodes with lower ECT s will be more likely to receive innovative packets (i.e., increase the rank) earlier than other nodes. On the other hand, wormhole links will make some nodes receive innovative packets (i.e., increase the rank) much earlier that they should. Thus, in the proposed centralized algorithm, we explore the order of rank increments in order to detect the wormhole links.

Basically, in RLNC, when an innovative packet is sent from the source node, the nodes near the source node are more likely to receive the innovative packets earlier than the nodes that are far from the source node. Also, we have demonstrated ECT is a proper metric to measure the distances between each node and the source node. Thus, the nodes with low ECTs can probably receive the innovative packets earlier. However, the existence of wormhole link intuitively changes the normal network topology since the innovative packets can be transmitted through the wormhole link directly and safely, and thus the nodes around the remote side of the wormhole link can receive the novel packets earlier than expected. With a wormhole link, the order of the rank increments among the nodes will be significantly changed .To illustrate the significant changes, we have a RLNC simulation For the centralized algorithm, we set up a central node, which owns the authority to gather information from all the nodes in the network, and we run a wormhole detection algorithm based on the rank increasing information on the central node. Each node is responsible to record the time when the rank of the received packets increases and then generates a report, which includes the details such as the time, the node address, and the rank. Each node delivers the reports to the central node via common unicast.

Based on the intuitions above, we propose Algorithm 1, the centralized algorithm to detect wormhole attacks on the central node. In Algorithm 1, the central node chooses an event of rank change, i.e., the rank increment from i to i + 1, and then searches the received reports to find all the related ones. Then we compare the time order of ECTs with the ascending ECT sequence and calculate the distance between them. If the distance exceeds the threshold, we decide there exists wormhole attack, and release the warning. At last, we update the bound of the distance for the next detection, in order to make our algorithm adaptive.

Algorithm 1: The Centralized Algorithm
Input: T: the reports from all the nodes V in the network G, D: the number of dimensions of the code vector space, Normal: the normal distance, Threshold: the threshold of alert
Output: whether there exists a wormhole attack in the network G, the updated Normal.
Step 1: Randomly select a rank r s.t. r ≥1 and r should be small enough, i.e., 1<=r<=5
Step 2: Let T_r be the set of the reports whose rank increments are from r -1 to r.
Step 3: Sort T_r into a sequence T_r^e s.t. the values of ECT in T_r^e are ascending.
Step 4: Let Le be the sequence of ascending ECTs in T_r^e .
Step 5: Sort T_r into a sequence T^t_r s.t. the values of time in T^t_r are ascending.
Step 6: Let L_t be the sequence of ECTs in T^t_r while preserving the order.
Step 7: Distance <--- Calculate - Distance (Le, Lt, |V |)
Step 8: if Distance -Normal > Threshold then
Step 9: Find out the addresses of the nodes with the most aberrant ECTs.
Step 10: Release a warning of wormhole attack.
Step 11: end if
Step 12: Update the value of Normal using k-means.

In Algorithm 1, each report t is a tuple as Equation (3): t = (time, addr, ECT, rank, $K_{pub,}$ sig) (3) Here, time denotes the time stamp of the rank increment; addr denotes the address of the node who sends the report; ECT is the ECT of the reporting node; the value rank means the rank increased from rank - 1 to rank. K_{pub} is the public key of the reporting node. sig is the digital signature of the report. The signature can be calculated by hashing function to obtain the abstract of the plain data P = (time, addr, ECT, rank, K_{pub}) and then encrypt the abstract using secret key K_{sec} of the local node. The result is the signature sig. In Algorithm 1, Tr denotes the set of the reports of rank increment from r -1 to r.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 08, August - 2017

B.THE DISTRIBUTED DETECTION ALGORITHM

We consider a practical scenario where centralized authority cannot be found. We propose DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems. The basic idea of DAWN is based on the two neighbor nodes u and v in the network satisfying ECT (u) < ECT (v),. For any two nodes in the neighborhood, the one with lower ECT is supposed to receive novel packets earlier than the other one with high probabilities. In other words, innovative packets are transmitted from low ECT nodes to high ECT nodes with high probabilities. In order to monitor the innovative packets transmission direction, nodes will work collaboratively. In particular, DAWN has two phases on each node: 1) Report packets direction observation results to its neighbors (Algorithm 2) Detect whether any attackers exist (Algorithm 3). The Detect phase is based on the received results from neighbors during the Report phase. Both of the algorithms are running on every node in the network. Algorithm 2 runs simultaneously while passing on the packets, and Algorithm 3should be asynchronous for different nodes and run at random time slots.

Algorithm 2 Report Function

Input: N (u) the set of u's neighbors; the number of the novel packets u received from each neighbor in the last batch; d: the threshold on ECT difference.

Output: s_v the local observation result for each neighbor v € N (u) Report messages if any.

Step 1: **for** v € N (u) **do**
Step 2: Denote p_v the number of novel packets that u received
From v during the last batch
Step 3: **if** ECT (v) –ECT (u) δ AND $p_v > 0$} then
Step 4: u broadcasts the report r (u, v, 0)
Step 5: Note r (u, v, 0) represents the report sent from u about
Suspicious wormhole behavior of v, with hop count 0.
Step 6: $s_v = 1$;
Step 7: **else**
Step 8: $s_v = 0$;
Step 9: **end if**
Step 10:**end for**

Report phase. As shown in Algorithm 2, for each node, it will suspect that one neighbor is an attacker if it receives novel packets from the neighbor but the ECT of this neighbor is much higher than that of itself (i.e., the distance between the ECTs is greater than the threshold d). It sends its judgment as a report to its neighbors.

Algorithm 3: The Distributed Detection Algorithm for Wormholes in Wireless Network Coding Systems (DAWN) on Node u

Input: R: the set of reports received in the last batch, N (u): the set
of u's neighbors, s_j: the local observation result of each neighbor j € N(u), d: the threshold.

Output: Detected wormhole attackers in N (u), if any.
Step 1: **for** each report r (i, j, k) € R **do**
Step 2: if ECT (j) – ECT (i) ≤ δ OR i ∉ N (j) then
Step 3: Discard this report;
Step 4: **else**
Step 5: **if** j € N (u) then
Step 6: s_j<--- s_j + 1
Step 7: **end if**
Step 8: if k < 2 then
Step 9: Forward this report r (i, j, k +1);
Step 10:**end if**
Step 11: **end if**
Step12: **end for**
Step 13: **for** each v € N (u) **do**
Step 14: Let C (v) = {i | i € N (v) s.t. ECT (v) – ECT (i) δ
Step 15: **if** s_v ≥ [| C (v) | +1 / 2] then
Step 16: Mark v as a detected wormhole attacker, and block any traffic from or to node v in future batches.
Step 17: **end if**
Step 18: **end for**

Detect phase. Algorithm 3 presents the pseudocode of the Detect phase of DAWN. For each node in the Detect phase, it receives reports from the judge nodes of any potential attackers. It first examines whether a report is from a valid judge node. If so, it will forward the report unless it has already been forwarded twice. Three-hops of the reports make sure that more (reachable) neighbors of the potential attacker will hear this report The detection algorithm on each node accumulates and calculates the number of its judge nodes who send report about the reported potential attacker in the current batch. If the number of judge nodes compose the majority, the node will make the decision that the attacker is involved in a wormhole attack and block it from future communications.

IV SIMULATION ENVIRONMENT

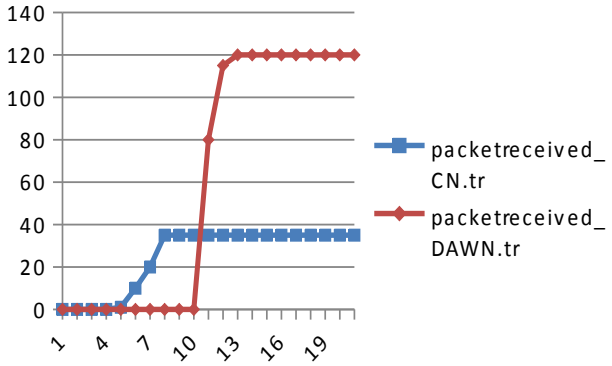
Channel	Channel/wireless
propagation	Propagation/two ray ground
Network interface	Phy/wireless Phy
Platform	Ubuntu 15.04
Ns version	Ns-allinone-2.35
MAC	Mac/802_11
Interface queue	Queue/drop tail/pri queue
Link layer	LL
Antenna	Antenna/omi antenna
Interface queue length	50
Number of nodes	36
Simulation area size	1000*900
Routing protocol	AODV
Simulation time	20 seconds
Traffic pattern	CBR

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 08, August - 2017

V SIMULATON RESULTS

Performance Evaluation

In this section, evaluate the performance of simulation. We are using the x graph for evaluate the performance. We choose the some evaluation metrics: Packet received ratio – the ratio of the total number of packets received by the destination node to the number of packet sent by the source, and also calculate the Packet Loss Ratio and End to End Delay. Along these evaluation metrics we have to evaluate the simulation performance in x graph.



Packet Received Ratio:

Fig 5.1 graph of Packet Received with Existing and Proposed Scheme

Packet Loss Ratio:

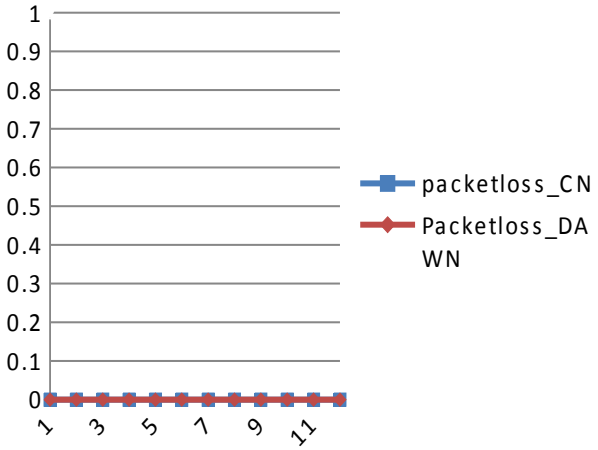


Fig 5.2graph of Packet Loss with Existing and Proposed Scheme.

End to End Delay:

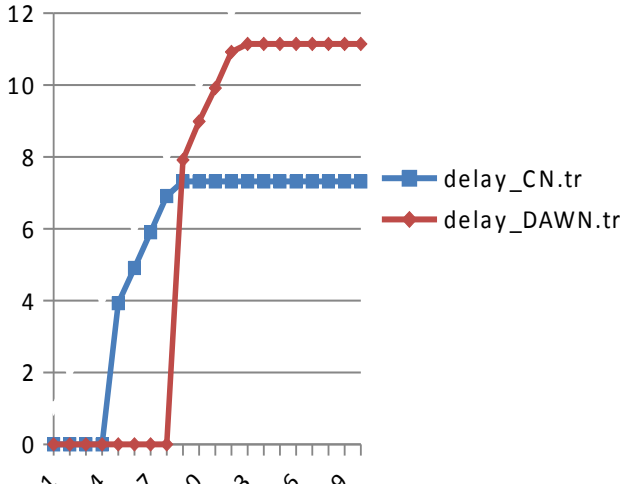


Fig 5.3 graph of Delay with Existing and Proposed Scheme.

VI CONCLUSION

In this work, we have investigated the negative impacts of wormhole attacks on wireless network coding systems. We have proposed two algorithms that utilize the metric ECT to defend against wormhole attacks. We have proposed a Centralized Algorithm that assigns a central node to collect and analyze the forwarding behaviors of each node in the network, in order to react timely when wormhole attack is initiated. We have proven the correctness of the Centralized Algorithm by deriving a lower bound of the deviation in the algorithm. We have also proposed a Distributed detection Algorithm against Wormhole in wireless Network coding systems, DAWN. DAWN is totally distributed for the nodes in the network, eliminating the limitation of tightly synchronized clock. DAWN is efficient and thus it fits for wireless sensor network. For both centralized and distributed algorithms, we have utilized the digital signatures to ensure every report is undeniable and cannot be forged by any attackers. The simulations have shown that the pro-posed algorithms can detect the malicious nodes participating in wormhole attack with high successful rate and the algorithm is efficient in terms of computation and communication overhead.

REFERENCES

[1] S. Li, R. Yeung, and N. Cai, “Linear network coding,”IEEE Trans.Inf. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[2] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B.Leong, “A random linear network coding approach to multicast,”IEEETrans. Inf. Theory, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[3] S. Biswas and R. Morris, “Opportunistic routing in multihop wireless networks,” ACM SIGCOMM Comput. Commun. Rev., vol. 34,pp. 69–74, Sep. 2004.

[4] S.Katti,H.Rahul,W.Hu,D. Katabi,M.Medard,and J.Crow-croft, “XORs in the air: Practical wireless network coding,” in Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun.,2006, pp. 243–254.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 08, August - 2017

[5] S. Chachulski, M. Jennings, S. Katti, andD. Katabi, "Trading structure for randomness in wireless opportunistic routing," in Proc.Conf. Appl., Technol., Archit. Protocols Comput. Commun., Aug. 2007,pp. 169–180.
[6] D. Dong, Y. Liu, X. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks,"IEEE Trans.Netw., vol. 19, no. 6, pp. 1787–1796, Dec. 2011.
[7] J. Kim, D. Sterne, R. Hardy, R. K. Thomas, and L. Tong, "Timing-based localization of in-band wormhole tunnels in MANETs," in Proc. 3rd ACM Conf. Wireless Netw. Security, 2010, pp. 1–12.
[8] S. R. D. R. Maheshwari, J. Gao, "Detecting wormhole attacks in wireless networks using connectivity information," inProc. IEEE 26th Int. Conf Commun., 2007, pp. 107–115.
[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks,"IEEE J. Sel. Areas Commun., vol. 24, no. 2,pp. 370–380, Feb. 2006.
[10] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," Wireless Netw., vol. 13, no. 1, pp. 27–59, 2007.
[11] A. J. Newell, R. Curtmola, and C. Nita-Rotaru, "Entropy attacks and countermeasures in wireless network coding," in Proc. 5th ACM Conf. Security Privacy Wireless Mobile Netw.,2012, pp. 185–196.
[12] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles," Wireless Commun. Mobile Comput., vol. 6, no. 4, pp. 483–503, Jun.2006.
[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," inProc. IEEE 23rd Annu. Joint Conf. IEEE Comput. Commun., Mar. 2003, pp. 1976–1986.
[14] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," inProc. 3rd ACM Workshop Wireless Security, Oct. 2004, pp. 51–60.
[15] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. IEEE Int. Conf. Netw. Protocols, 2006,pp. 75–84.
[16] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Sector: Secure tracking of node encounters in multi-hop wireless networks," inProc. 1st ACMWorkshop Security Ad Hoc Sensor Netw., 2003, pp. 21–32.
[17] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," Wireless Netw., vol. 11, no. 4, pp. 419–434, 2005.
[18] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage sys-tems," IEEE Trans. Inf. Theory,vol. 56, no.9,pp.4539–4551,Sep. 2010.
[19] A. S. Avestimehr, S. N. Diggavi, and D. N. Tse, "Wireless network information flow: A deterministic approach,"IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.
[20] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," IEEE Trans. Inf. Theory,vol. 57, no. 10, pp. 6463–6486, Oct. 2011.
[21] P. Santi, "Topology control in wireless ad hoc and sensor networks,"ACM Comput. Surv., vol. 37, no. 2, pp. 164–194, 2005.
[22] F. Wu, T. Chen, S. Zhong, L. E. Li, and Y. R. Yang, "Incentive-compatible opportunistic routing for wireless networks," inProc. 14th ACM Int. Conf. Mobile Comput. Netw., 2008, pp. 303–314.
[23] S. Lloyd, "Least squares quantization in PCM," IEEE Trans. Inf. Theory, vol. IT-28, no. 2, pp. 129–137, Mar. 1982.
[24] C. Cortes and V. Vapnik, "Support vector machine,"Mach. Learn., vol. 20, no. 3, pp. 273–297, 1995.
[25] W. Hoeffding, "Probability inequalities for sums of bounded random variables,"J. Amer. Statist. Assoc., vol. 58, no. 301, pp. 13–30,1963.
[26] Beecrypt
[27] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems,"Commun. ACM,vol. 21, no. 2, pp. 120–126, 1978.
[28] R. Rivest, "The md5 message-digest algorithm," RFC 1321, 1992.