Vulnerability Evaluation of Network Traffic Using Set Theoretic Analysis for Joint Security and Routing

[1]R.Naresh and [2]P. Selvakumar

[1]*R.NARESH is with M.E student, G.K.M College of Engineering & Technology, Alapakkam –Mappedu Road, G.K.M Nagar, Chennai-63, and India. Email: naresh_it07@yahoo.co.in*

[2] *P.SELVAKUMAR is with, Asst. Professor, Department of Computer Science & Engineering, G.K.M College of Engineering & Technology, Alapakkam –Mappedu Road, G.K.M Nagar, Chennai-63, and India. Email: p_selvakumar2005@yahoo.co.in*

***Abstract*—The routing protocols in the wireless networks disclose the fact that security and routing cannot be established jointly. Investigation is done on the impact of node capture attacks on the confidentiality and integrity of network traffic. I develop a method called GNAVE (Greedy Node capture Approximation using Vulnerability Evaluation) to maximize the vulnerability resulting from the capture of each individual nodes using the information required form the previously captured node which jointly provides the security using RVM (Route Vulnerability Metric) method which quantifies the effective security of traffic traversing for a given node as well as the optimized routing using set theoretic analysis. The vulnerability is measured using routing and cryptographic protocols for the analysis of weakness in every node and provides secured network traffic. The minimum cost node capture attack is evaluated at every point of time. Using the known parameters like bandwidth, channel capacity, mobility speed the adverse effects can be analyzed. Key management facility is embedded as a part of this project. A key management scheme is designed which satisfy the security requirements by selectively distributing the keys to the nodes without overhead of computations or bandwidth usage.**

***Index Terms*—Wireless networks, security, routing, node capture attacks, adversary models.**

1 INTRODUCTION

Assurance of secure applications and services in wireless networks relies on the properties of confidentiality and integrity, respectively defined as the ability to keep data secret from unauthorized entities and the ability to verify that data has not been maliciously or accidentally altered [2].Eschenauer and Gligor recently demonstrated in [3] that these properties can be efficiently compromised by physically capturing network nodes and extracting cryptographic keys from their memories. These node capture attacks are possible in most wireless networks due to the unattended operation of wireless nodes and the prohibitive cost of tamper-resistant hardware in portable devices [3]. Further-more, as shown in [4], an intelligent adversary can improve the efficiency of a node capture attack over that of approaches in recent literature [3], [5], [6], [7] focusing on random node capture using publicly available information leaked from the key assignment protocol.

The aforementioned studies on node capture attacks have all focused on the ability of an adversary to compromise the security of single-hop wireless links. However, messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing a single insecure link The overall security of routed messages is thus dependent on the routing protocol implemented in the wireless network, as well as the physical network topology and the relative positions of the source and destination nodes in the network. Moreover, the fact that a message is transmitted over numerous links between a source and destination node implies that the overall confidentiality and integrity of the routed message may only be as secure as the least secure link, implying that vulnerabilities arise due to the topology of secure links in the wireless network. Hence, the impact of a node capture attack is a function of both the cryptographic protocol which provides link security and the routing protocol which determines the set of links traversed by a given message. In this article, we introduce a class of metrics to measure the effective security offered in a wireless network as a function of **Our Contributions**

We make the following contributions in this article:

- We define a class of metrics for the vulnerability of network traffic and formulate the minimum cost node capture attack problem as a nonlinear integer program using the defined vulnerability metrics. We present the GNAVE algorithm,a Greedy Node capture Approximation using Vulnerability Evaluation, to approximate the minimum cost node capture attack.
- We provide two complementary realizations for the Vulnerability metric by interpreting the compromise of messages using set theoretic and

circuit theoretic analogies to evaluate the message security.

- We show that when information about the key assignment protocol is hidden from the adversary using privacy-preserving protocols, the indeterminate quantities can be estimated probabilistically without significant degradation in the attack performance.
- We demonstrate the impact of node capture attacks using the GNAVE algorithm in wireless networks with examples of both classical routing and network coding protocols. Furthermore, we compare the resource expenditure required for node capture attacks using the GNAVE algorithm to previously proposed strategies via simulation.

2 MODELS AND NOTATION

In this section, we state the assumed wireless network, key assignment, and adversary models. We summarize the notation used throughout this article in Table 1.

2.1 Network Model

The topology of the wireless network with a set of nodes N is represented by the directed network graph G =(N,L).The link set L contains all ordered pairs of one-hop communicating neighbors, equivalent to an asymmetric relation[10], such that (i,j) is in L for i≠ j if and only if node i can reliably send messages to node j without intermediate relay nodes. The link set L is dependent on parameters such as node location and configuration and properties of the radios, transmission medium, and MAC layer protocols.

We denote the subsets of N of message source and destination nodes in the network as S and D, respectively. The set of source-destination pairs is denoted T≤ S x D and is constructed based on the routing protocol decisions.

For a given source-destination pair(s,d) € T , the routing protocol will construct one or more directed routing paths through G, where a path is defined as a set of sequential links in L. We define route R_{sd} as the set of all paths traversed by any message from s to d, and we let f denote the fraction of traffic from s to d that traverses the given path π € R_{sd}. The route R_{sd} can be represented graphically by the route subgraph G_{sd} of G consisting of nodes and directed links traversed by at least one routing path π € R_{sd} from s to d.

2.2 Key Assignment Model

We assume the existence of a secure key assignment mechanism as follows: Let K be a set of symmetric cryptographic keys and L be a corresponding set of publicly available key labels. Each node I € N is assigned a subset $K_i \leq K$ and the corresponding subset $L_i \leq L$. We denote the subset of keys shared by nodes i and j as $K_{ij=} K_{i\cap} K_j$ and allow communication between i and j if and only if $K_{ij=0}$.[1]We assume that nodes i and j use the entire set K_{ij} of shared keys to secure the link (i, j), so the strength of the link security is directly related to the number of shared keys. We assume that nodes i and j compute the intersection $L_{ij=} L_{i\cap} L_j$ in order to determine the set of shared keys K_{ij} using a protocol from one of the following classes.

2.3 Adversarial Model

We consider a polynomial-time adversary with the ability and resources to eavesdrop on and record messages throughout the network, capture nodes, and extract cryptographic keys from the memory of captured nodes. We assume that the adversary has knowledge of the key assignment and routing protocols, including protocol parameters, and can participate actively in any network protocols by assuming the roles of captured, replicated, or fabricated nodes. We further assume that the route subgraph G_{sd} for each (s, d) Є T is available to the adversary or is computable using traffic analysis and Estimation [18].

3. ROUTE VULNERABILITY METRICS UNDER NODE CAPTURE ATTACKS

In this section, we define a class of route vulnerability metrics (RVMs) to quantify the effective security of traffic traversing a given route R_{sd}. Using the RVM definition, we formulate the minimum cost node capture attack problem as a nonlinear integer programming minimization problem. Since determining the optimal node capture attack is likely infeasible, we propose the GNAVE algorithm using a greedy heuristic to iteratively capture nodes which maximize the increase in route vulnerability

3.1 Route Vulnerability Metric (RVM)

In order to evaluate the effect of a node capture attack on the effective security of traffic traversing a routeR_{sd}, we formally define link, path, and route compromise due to the capture of a subset C≤N of network nodes. We denote the set of keys recovered by the adversary in capturing the subset C as $K_{C=Ui\text{Є}CnK}$i If a message traverses a link which is secured by keys in K_C, the security of the message is compromised. The compromise of individual links in the network, with respect to the network and routing models in Section 2, is defined as follows:

3.2 Node Capture Attack Formulation

For any RVM realization satisfying the conditions of Definition 8, we devise a node capture strategy that maximizes the progression toward the goal of compromising all routes R_{sd} for (s,d) Є T_A. The choice of subset C requiring the minimum resource expenditure is thus given by the following minimum cost node capture problem.

Problem: Minimum Cost Node Capture Attack
Given: $\mathcal{L}_i$, w_i for $i \in \mathcal{N}$, $\mathcal{R}_{sd}$ for $(s,d) \in \mathcal{T}_A$
Find: $\mathcal{C} \subseteq \mathcal{N}$
such that $\sum_{i \in \mathcal{C}} w_i$ is minimized
and $V_{sd}(\mathcal{C}) = 1$ for all $(s,d) \in \mathcal{T}_A$.

In general, based on Definition 6 of path compromise, the metric V_{sd} (C) is nonlinear in the entries of C. Hence, the minimum cost node capture attack above is a nonlinear integer programming minimization problem, known to be NP-hard [10], [19]. We thus propose the use of a greedy heuristic that iteratively adds nodes to C based on maximizing the increase in route vulnerability V_{sd} (C) at each step. The heuristic is thus similar to a known greedy heuristic for set covering [20] and linear integer programming [19]. However, due to the nonlinearity in V_{sd}(C), the worst-case performance of the greedy heuristic cannot be analyzed using the ratio-bound analysis in [10], [19], [20] and is left as an open problem. To maximize the route vulnerability V_{sd} (C) with minimum resource expenditure, it is beneficial to the adversary to attempt to maximize the vulnerability resulting from the capture of each individual node using the information recovered from previously captured nodes. The contribution of a node i is thus given by the increase in route vulnerability V_{sd}(C U {i}) – Vsd(C) due to the addition of i to C. Allowing for an additional weight sd to indicate the adversary's preference to compromise the route R_{sd} over other routes, the value of each node i is defined as follows:

To maximize the cost effectiveness of the node capture attack at each iteration, the adversary chooses to capture the node with maximum incremental value per unit cost V_i(C) /w_i. Based on this greedy approach, we propose the GNAVE algorithm as follows:

The adversary thus captures nodes intelligently by associating an individual weight or cost w_i with the resource expenditure required to capture each node i 2 N , as in [4]. We do not address further attacks on network protocols and services that can be performed as a result of message compromise.

GNAVE Algorithm

Given: $\mathcal{L}_i$, w_i for $i \in \mathcal{N}$, $\mathcal{R}_{sd}$ for $(s,d) \in \mathcal{T}_A$
$\mathcal{C} \leftarrow \emptyset$
while there exists $(s,d) \in \mathcal{T}_A$ with $V_{sd}(\mathcal{C}) < 1$ **do**
  $i^* \leftarrow \operatorname{argmax}_{i \in \mathcal{N}} \nu_i(\mathcal{C})/w_i$
  $\mathcal{C} \leftarrow \mathcal{C} \cup \{i^*\}$
end while

4 RVM REALIZATIONS

In this section, we propose two RVM realizations satisfying the conditions in Definition 8, noting that there is a high degree of freedom in the given conditions. We present each RVM realization for each of the routing protocol classes discussed in Section 2.1, hereafter denoting the route vulnerability for independent and dependent path routing protocols as respectively. The definitions presented in this section are derived using the following necessary and sufficient condition for the compromise of a route R_{sd} with respect to the edge cuts of the route subgraph G_{sd}.

Theorem 1. The route R_{sd} is compromised if and only if the set L_C of compromised links contains at least one (s, d) edge cut of the route subgraph G_{sd} as a subset.

5 SET THEORETIC VERSION OF RVM

We formulate a set theoretic RVM realization V_{sd} (C)$_{SET}$ by interpreting the properties of edge cuts of G_{sd} set theoretically. From Theorem 1, the existence of a compromised edge cut set $L_{cut} \leq L_c$ of the route subgraph G_{sd} implies that the route R_{sd} is compromised. In terms of the set K_c of compromised keys, a necessary and sufficient condition for L_c to contain an edge cut set of Gsd is However, this function does not satisfy the third condition of Definition 8 as the resulting function does not take continuous values between 0 and 1.The above formulation provides insight into the route vulnerability, however, suggesting that a valid RVM can be obtained with minor modifications. First, to ensure that any compromised path is accounted for in the vulnerability evaluation, the product over all paths in R_{sd} can be replaced by a weighted summation over the corresponding paths, including the secure end-to-end link (s,d) as a single-hop path. We denote the relative weight assigned to the secure end-to-end link (s,d) as f_{sd} with the assumption that $f_{sd} > 0$ is allowed to vary arbitrarily when the additional end-to-end secure link is used and that $f_{sd} = 0$ otherwise, thus impacting the choice of captured nodes. We relax the binary condition imposed by the indicator function $1(K_{ij} \leq K_C)$ by the function $\varphi_{ij}(C)$ equal to the fraction of keys in K_{ij} that are contained in K_C, given by for the secure end-to-end link(s,d) Applying this relaxation to the right-hand side of (1) thus yields the following RVMs for independent and dependent path routing protocols, which vary only in the weighting of individual paths in R_{sd}.

For independent path routing protocols, the compromise or independent path routing protocols, the compromise of an individual path $\pi \epsilon R_{sd}$ is sufficient to allow the adversary to recover a fraction f_π of the traffic from s to d. applying the continuous relaxation to the right-hand side of (1) for each single path route in R_{sd} and summing over the single path routes with corresponding weights f, including the end-to-end link (s,d) with weight f_{sd}, yields the RVM for independent path routing protocols as

6 CONCLUSION

In this article, we investigated the problem of developing new vulnerability metrics that improve the efficiency of node capture attacks when the routing and key assignment protocols used in a wireless network are jointly analyzed We proposed a class of route vulnerability metrics (RVMs) to evaluate the effect of node capture attacks on secure network traffic and developed two RVM realizations using set and circuit theoretic interpretations of the compromise of secure network traffic. We formulated the optimal node capture attack using RVM evaluation as a nonlinear integer programming minimization problem and presented the GNAVE algorithm using a greedy heuristic to approximate the NP-hard problem. We demonstrated a probabilistic approach to estimate the route vulnerability when privacy preserving set intersection protocols are used to hide information from the adversary. Finally, we illustrated node capture attacks using the GNAVE algorithm and compared the performance of the GNAVE algorithm with previously proposed node capture strategies. We provided simulation results to demonstrate the performance gains in using the circuit theoretic RVM, noting that similar results not included in this article have been obtained using the set theoretic RVM. In the future, the node capture attack framework proposed in this article will assist in the joint design of key assignment and routing protocols for wireless networks that are robust to node capture attacks.

REFERENCES

[1] Eschenauer.L and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks,"Proc. Ninth ACM Conf. Computerand Comm. Security (CCS '02), pp. 41-47, Nov. 2002.

[2] Tague,.p D. Slater, J. Rogers, and R. Poovendran, "Vulnerability of Network Traffic Under Node Capture Attacks Using Circuit Theoretic Analysis," Proc. IEEE INFOCOM '08,pp. 664-672, Apr. 2008.

[3] Tague.P and R. Poovendran, "Modeling Adaptive Node Capture Attacks in Multi-Hop Wireless Networks," Ad Hoc Networks, vol. 5, no. 6, pp. 801-814, Aug. 2007.

[4] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks,"Proc. IEEE Symp. Security and Privacy (SP '03), pp. 197-213, May 2003.

. [5] W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," ACM Trans. Information and System Security, vol. 8,no. 2, pp. 228-258, May 2005

[6] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," ACM Trans. Information and System Security, vol. 8, no. 1, pp. 41-77, Feb. 2005.

[7] N. Cai and R.W. Yeung, "Secure Network Coding," Proc. IEEE Int'l Symp. Information Theory (ISIT '02), p. 323, June/July 2002.

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

[9] C. Schurgers ,M.B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks,"Proc. Military Comm. Conf.(MILCOM '01),pp. 357-361, Oct. 2001.

[10] M. Ramkumar and N. Memon, "An Efficient Random Key Pre-Distribution Scheme," Proc. IEEE Conf. Global Comm.(GLOBECOM '04), pp. 2218-2223, Nov./Dec. 2004.