PROBABILISTIC APPROACH FOR VULNERABILITY ANALYSIS USING GNAVE ALGORITHM FOR NODE CAPTURE ATTACKS IN WSN

Manjula H.T[1], Amreen Khanam[2], Sumathi D[3]

[1, 2, 3] *Asst Prof, Dept. of CSE, HKBK College of Engineering, (India)*

ABSTRACT

The impact of node capture attacks on the confidentiality and integrity of network traffic, where it is attempted to map the compromise of network traffic to the flow of current through an electric circuit and propose a metric for quantifying the vulnerability of the traffic using the circuit mapping. It computes the vulnerability metric as a function of the routing and the cryptographic protocols used to secure the network traffic and formulate the minimum cost node capture attack problem as a nonlinear integer programming problem. Due to the NP-hardness of the minimization problem, a greedy heuristic is implemented that approximates the minimum cost attack by providing examples of node capture attacks using the vulnerability metric and show that the adversary can expand significantly less resources to compromise target traffic by exploiting information leakage from the routing and cryptographic protocols. Finally, the framework is targeted to design where it can formalize node capture attacks using the vulnerability metric as a nonlinear integer programming minimization problem and with the proposed GNAVE algorithm, a Greedy Node capture Approximation using Vulnerability Evaluation with a discussion on the availability of security parameters to the adversary and show that unknown parameters can be estimated using probabilistic analysis.

Index Terms: Wireless Networks, Security, Routing, Node Capture Attacks, Adversary Models.

I. INTRODUCTION

The successful commercialization of many applications of wireless networks relies on the assurance of the confidentiality and integrity of the data communicated through the network. Confidentiality is defined as the ability to keep data secret from all but a set of authorized entities, and integrity is defined as the ability to verify that data has not been maliciously or accidentally altered while in transit. It has demonstrated that these properties can be efficiently compromised by physically capturing network nodes and extracting cryptographic keys from their memory. Such node capture attacks are possible due to the potential unattended operation of wireless nodes and the prohibitive cost of tamper-proof hardware in portable devices. Using the cryptographic keys recovered in a node capture attack, an adversary can compromise the confidentiality and integrity of any messages secured using the compromised keys .For symmetric key assignment in wireless sensor and adhoc networks, node capture attacks aim at the compromise of individual node-to-node wireless links. However, a message traversing multiple links between a source and destination node is compromised if any of the traversed links in the route becomes insecure. The overall security of a routed message is thus at best that of the least secure or most vulnerable link traversed by the message. Hence, the impact of the node capture attack is a function of both the cryptographic protocol which provides link security and the routing protocol which determines the links traversed by a given message.

II. RELATED WORK

In [1] they mapped compromise of network traffic to the flow of current through an electric circuit and formulated the minimum cost node capture attack as a nonlinear integer programming minimization problem using the route vulnerability metric and provided a greedy heuristic solution called GNAVE to approximate the NP-hard minimization problem and showed that an adversary can significantly decrease the resource expenditure by intelligently capturing nodes using the proposed route vulnerability metric.

In [2] they presented a new key management scheme for large- scale DSNs. This approach was scalable and flexible. They illustrated the effect of modifying design parameters using both analysis and simulations.

In [3], they investigated the problem of modeling node capture attacks in heterogeneous wireless ad hoc and mesh networks. It is shown that probabilistic heuristic attacks can be performed effectively even under storage randomization.

In [4]&[5] Pairwise key establishment was used as a fundamental security service in sensor networks, which enables the sensor nodes to communicate securely with each other using cryptographic techniques

In [7] they derived a practical guideline based on the energy histogram and developed a spectrum of new techniques to enhance the routing in sensor networks.

In [8] they showed that attacks in adversary model correspond to NP-hard optimization problems and discuss the behavior of a reasonable heuristic algorithm. They demonstrated the use of the attack decomposition model for derivation of attack metrics and discuss the potential use of this decomposition technique for the purposes of defense against node capture attacks.

III. EXISTING SYSTEM

The previous studies on node capture attacks focused on the ability of an adversary to compromise the security of single-hop wireless links. Messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing insecure link. A symmetric key assignment for resource-constrained devices has focused on node capture attacks in which an adversary chooses the captured nodes independently at random.

- In the existing system, it is seen that an intelligent adversary can reduce the resource expenditure required for the node capture attack using information leaked from the key assignment protocol.
- In particular, the adversary can learn which keys are assigned to individual nodes in the network by eavesdropping on or participating in the secure link establishment protocol and are also based on the single mission-key solution which is inadequate because the capture of any sensor node may compromise the entire DSN since selective key revocation is impossible upon sensor-capture detection.
- Pair wise keys [4] allow for secure key establishment with low complexity, but the storage requirement of (N-1) pair wise keys for each of the N nodes may be prohibitive for large networks.

IV. PROPOSED WORK

To address the problems and the issues in existing system, the vulnerability of network traffic is used as a measure of the adversary's ability to compromise a message traversing a particular route in the given framework (WSN).

4.1 Advantages of the Proposed System

- Node capture attacks result from the combination of passive, active, and physical attacks by an intelligent adversary.
- To initialize or set up an attack, the adversary will collect information about the WSN by eavesdropping on message exchanges, either local to a single adversarial device or throughout the network with the aid of a number of adversarial devices deployed throughout the network.
- Even if message payloads are encrypted, the adversary can extract information about the network operation and state, effectively learning about the network structure and function.
- In addition to passive learning, the adversary can actively participate in network protocols, probing the network for information and maliciously injecting information into the network.
- Once a sufficient amount of passive and active learning has taken place, the adversary can physically capture nodes.
- The gathered information can be used to help the adversary make an informed decision of which sensor nodes to capture in order to optimize the performance of the attack with respect to a specific attack goal.

4.2 Network Setup Module

The network simulation environment is developed here where constant bit rate traffic sources will be used. The radio model in the simulator will be based on Linksys WLAN 802.11 providing an optimum transmission rate. The link layer model will be simulated in IEEE 802.11 WLAN standard where a 15-20 mode network in a field with approximate dimensions of 670x670 will be used. The source-destination pair are separated randomly over the network. A specific data byte packet will be used where simulations are run for 500 simulated seconds. The major objective of design of the network setup module is to discover certain important network parameters like:

1. Network Region.
2. Channel Capacity.
3. Transmission Range
4. Size of Data Packet.
5. Minimum Mobility Speed.
6. Maximum Mobility Speed.

4.3 Key Assignment Module

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 $i \in N$ is assigned a subset $K_i \subseteq K$ and the corresponding subset $L_i \subseteq L$. 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 $K_{ij} \neq 0$¸. 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 $Lij = L_i \cap L_j$ in order to determine the set of shared keys K_{ij} using a protocol from one of the following classes:

1. The class of public label exchange protocols consists of any protocol which provides necessary information for any node $j \in N$ to compute the set L_i of key labels for any node $i \in N$.
2. The class of privacy-preserving set intersection protocols consists of any protocol which provides necessary information for any node $j \in N$ to only compute the set L_{ij} of key labels shared with any node $i \in N$ without giving any information to j about the remaining key labels in $L_i \setminus L_j$

4.4 Adversarial Module

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 $(s,d) \in T$ is available to the adversary or is computable using traffic analysis and estimation.

The primary goal of the adversary is to compromise the confidentiality and integrity of all messages routed between a target set of source-destination pairs denoted $T_A \subseteq T$ by extracting cryptographic keys from the memory of captured nodes $C \subseteq N$ with minimum resource expenditure. The adversary thus captures nodes intelligently by associating an individual weight or cost w_i with the resource expenditure

required to capture node $i \in N$, We do not address further attacks on network protocols and services that can be performed as a result of message compromise

4.5 Node Capture Attack Formulation Module

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.

In order to evaluate the effect of a node capture attack on the effective security of traffic traversing a route R_{sd},we formally define link, path, and route compromise due to the capture of a subset $C \subseteq N$ of network nodes. We denote the set of keys recovered by the adversary in capturing the subset C as $K_C = U_{i \in N} K_i$. If a message traverses a link which is secured by keys in KC, the security of the message is compromised. The compromise of individual links in the network, with respect to the network and routing models. we devise a node capture strategy that maximizes the progression toward the goal of compromising all routes R_{sd} for $(s, d) \in A$. The choice of subset C requiring the minimum resource expenditure is thus given by the minimum cost node capture problem. To maximize the route vulnerability 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.

Based on this greedy approach, we propose the GNAVE algorithm as follows GNAVE Algorithm:

Given: L_i, w_i for $i \in N$, R_{sd} for $(s,d) \in T_A$

$C \leftarrow 0$

While there exists $(s,d) \in T_A$ with $V_{sd}(C) < 1$ do

$$I^* \leftarrow \arg\max_{i \in N} v_i(C)/W_i$$

$C \leftarrow C \cup \{i^*\}$

End while

[L]= Set of ordered pair of one-hop neighbor nodes

W=weight or cost of capturing nodes

R_{sd} =Set of paths forming the route from s to d

S=source

D=Destination

T_A=Adversary Target subset

C=Captured nodes

V_{sd} =Route Vulnerability

The GNAVE algorithm being greedy implies that the attack performance depends only on the order of the weighted node values for the nodes

4.6 Implementing RVM realizations Module

In this section, we propose two RVM realizations satisfying the certain conditions, 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 network model setup, hereafter denoting the route vulnerability for independent and dependent path routing protocols. The RVM here is represented by set theory as well as in circuit theory.

4.7 Comparison of RVM Realizations

We provide a pair of examples to illustrate cases in which the RVMs are evaluated using the provided definitions. Each of the examples demonstrates a scenario where one metric provides more information to the adversary in choosing which nodes to capture. Both examples are presented using the network for a source and destination with intermediate nodes. The number of shared keys for each link is also defined, and the costs to capture are assumed to be infinity. The other nodes present in the network have unit cost to capture and are of two types and the adversary must choose between two nodes by computing the node values using GNAVE algorithm

V. EXPERIMENTAL RESULTS

The following snapshots are some experimental results for vulnerability analysis using GNAVE algorithm for node capture attacks in WSN.

5.1 Network Setup Module

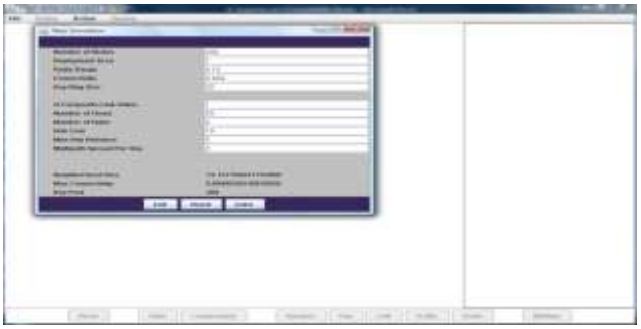

Figure : Setup Network Topology

This screen is used to pass the parameters so that the network will be constructed in the simulation mode such as the number of nodes, Deployment Area, Radio Range, connectivity, Key ring size, Q composite value, number of flows, number of hubs, hub cost, maximum hop distance, multipart spread per hop, neighborhood size, maximum connectivity, and key pool has to be defined and once the user select the enter button, number of nodes will be constructed in a network in the simulation mode.

5.2 Wireless Network Region

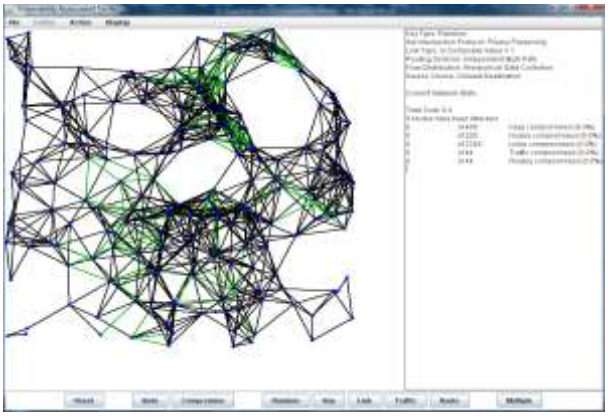

Figure: Wireless Communication Networks

This screen shows the nodes and links in a network. The right side in the figure shows the status of the network.

5.3 Key Assignment Module

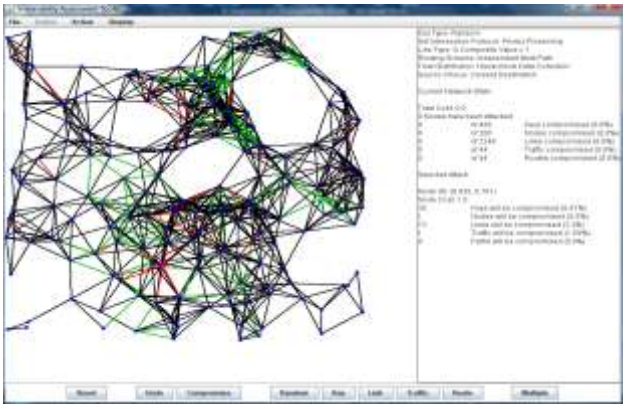

Figure : The Compromised Traffic and Paths

This screen shows the keys compromised, nodes compromised, links compromised, Traffic compromised, paths compromised.

5.4 Adversary Module

The figure below shows the user to initiate multiple nodes to be attacked in WSN the user has to enter multiple icons which is seen on the screen. We get a dialog box indicating the number of nodes to be attacked, user has to enter the number of nodes to be attacked, keys to be attacked, links to be attacked, traffic to be attacked, route to be attacked in a simulation node.

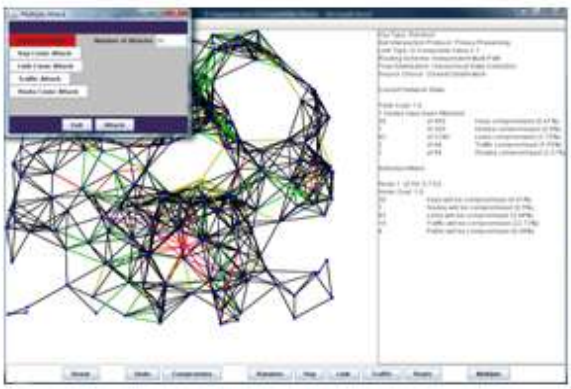

Figure : Initiates Multiple Attack

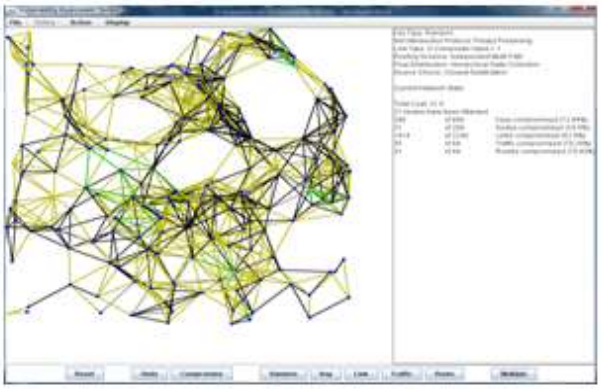

Figure: Multiple Nodes Compromised

This screen shows that when the user initiates multiple attacks the nodes compromised in the simulation mode .Once the user enters multiple attacks then all the nodes will be compromised in the simulation mode.

VI. CONCLUSION

In this paper we present the major contribution of the node capture attack using GNAVE algorithm in WSN. The probabilistic approach for vulnerability analysis using GNAVE algorithm for node capture attacks in WSN has the following unique features:

- Nodes are captured independently at random, serving as the baseline performance for the adversary.
- Nodes are captured iteratively to maximize the number of compromised keys by choosing the node with maximum at each iteration.
- Nodes are captured iteratively to maximize the number of compromised links by choosing the node which compromises the maximum number of additional links, independent of the routing protocol. Under privacy-preserving protocols, this attack uses the estimation techniques.
- Nodes are captured iteratively to maximize the amount of network traffic routed through captured nodes, independent of the key assignment protocol.
- Nodes are captured using the GNAVE algorithm and the RVM using information from both the routing and key assignment protocols.

REFERENCES

[1] Vulnerability of Network Traffic under Node Capture Attacks using Circuit Theoretic Analysis Patrick Tague, David Slater, Jason Rogers,and Radha Poovendran Network Security Lab (NSL), Electrical Engineering Department, University of Washington, Seattle, Washington, IEEE 2008

[2] A Key Management Scheme for Distributed Sensor Networks Laurent Eschenauer, Virgil D. Gligor Electrical and Computer Engineering Department University of Maryland College Park, MD, USA IEEE 2002

[3] Modeling adaptive node capture attacks in multi-hop wireless networks Patrick Tague, Radha Poovendran Network Security Lab (NSL), Department of Electrical Engineering, University of Washington IEEE 2007

[4] A Pairwise Key Predistribution Scheme for Wireless Sensor Networks Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney IEEE 2003

[5] Establishing Pairwise Keys in Distributed Sensor Networks Donggang Liu, Peng Ning Cyber Defense Laboratory Department of Computer Science North Carolina State University, IEEE 2003

[6] Secure Network Coding Ning Cai_and Raymond W. Yeungy: IEEE 2008

[7] Energy Efficient Routing In Wireless Sensor NetworksCurt Schurgers, Mani B. Srivastava Networked & Embedded Systems Lab (NESL), Electrical Engineering Department University of California at Los Angeles

[8] Modeling Node Capture Attacks in Wireless Sensor NetworksPatrick Tague and Radha Poovendran Network Security Lab (NSL), Electrical Engineering Department, University of Washington, Seattle, Washington Invited paper.