Research Proposal for Collaborative Research at Purdue University

Current approaches to deal with attacks on network systems handle individual attack at a time. Collaborative attacks are those that are launched by multiple attackers which synchronize their activities to harm the network in co-ordination with each other. Threats by collaborating attackers are much more complex, powerful and sophisticated. They render the solutions for single attacks ineffective. Coordinated attacks may cause more devastating impacts on a network as more than one attacker combine their efforts to harm the network. In this work, we propose to model the collaborative attacks and suggest defense against them.

Problem Statement

Mobile ad hoc networks rely on co-operation amongst devices that route packets for each other. Each device's data may pass through one or more not so friendly hands of other devices. These not so friendly nodes can do a lot of damage to the data/control packets. Moreover, lack of central controlling authority and the properties of wireless links make MANETs vulnerable to threats in security. Attacks range from passive eavesdropping in which the attacker may get access to secret information thereby violating the confidentiality to active impersonation, message replay, and message distortion. Attacks may be by an external source which is not a part of the network and hence does not have valid signatures or could be from a compromised node within the network.. Chances of a node being compromised in a hostile environment (e.g., a battlefield) with relatively poor physical protection are non-negligible.

The routing protocols for these networks such as AODV, DSR, and DSDV have been designed without considering security issues. In routing protocols like AODV where an intermediate node may reply to a route request with a route to destination, a malicious node responds positively to a request for a shortest route, even though it does not have a valid route to the destination node. Since the node does not have to check its routing table, it is the first one to respond to route discovery request in most cases. When the data packet sent by the source reaches the malicious node, it drops the packets rather than forwarding to the destination making a *black hole* there.

The mobile devices use a wireless medium to transmit information, the malicious nodes can eavesdrop the packets, tunnel them to another location in the network and retransmit them at the other end. The tunnel so created forms a *wormhole*. The tunneling procedure generates an illusion that the two nodes more than one hop away are in the neighborhood of each other. Since most of the route discovery mechanisms maintain a neighborhood set at each node, false information about a node's neighbor can severely affect the discovered route. If the routing protocol uses the number of hop-counts to compute the shortest path, it prevents the routes longer than three hops to be discovered.

In [36] Hu etal introduced first time rushing attack against on demand routing protocols. In routing protocols like AODV where an intermediate node processes route request packet received first and drops the succeeding ones, a malicious node rushes and

forwards a route request packet as fast as it can and thus diminish the possibility of establishing path through the legitimate nodes through which the request arrives a little later.

Generally two approaches are used to secure the routing protocols against these attacks. 1) local collaboration (Watchdog, CORE, CONFIDANT, Khalil etc): the neighboring nodes collectively monitor each other and generate reputation/trustworthiness of their neighbor nodes and inform other nodes in the network; and 2) information cross-validation: each node monitors its neighbors by cross-checking the overheard transmissions, and the monitoring results from different nodes are further cross validated. Sometimes the cross-validation is also done by sending *further request* and *further reply* (Deng, RAODV) packets to/from the next-hop/destination.

These approaches will fail when several nodes collude to manifest an attack. For example, an external node may collude with an internal node to generate good reputation for it thereby gaining access to the system. Two compromised nodes may collude to befool a cross-validation mechanism. In this work, we address the issues concerning these more powerful attacks. We intend to characterize, model and suggest solutions for such attacks.

Related Work

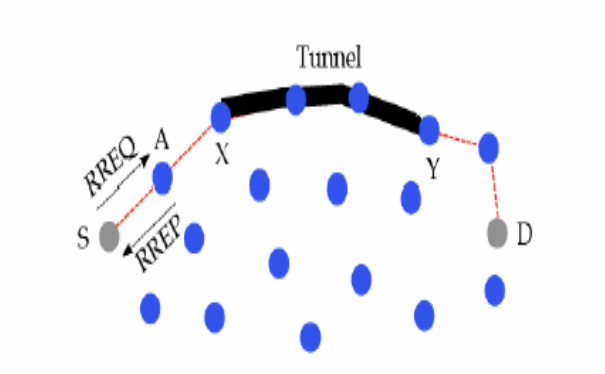
Attention of the researchers towards these devastating attacks is very recent. Not much work has been done in this direction but the efforts are on. Patcha and Mishra [PM03] have extended the *watchdog* [MGLB00] strategy to handle blackhole attacks by multiple nodes.

Ramaswamy etal [RFKN05] presented an algorithm in [5] which claims to prevent the cooperative black hole attacks in ad-hoc network. In this algorithm each node maintains an additional Data Routing Information (DRI) table. Whenever a node (say IN) responded to a RREQ it send the id of its next hop neighbor (NHN) and DRI entry for NHN to the source. If IN is not a trustable node for source then source sends a further route request (FRq) to NHN. NHN in turn responds with FRp message including DRI entry for IN, the next hop node of current NHN, and the DRI entry for the current NHN's next hop. If NHN is trusted node then source checks whether IN is a black hole or not using the DRI entry for IN replied by NHN. If NHN is not trustable node then the same cross checking will be continued with the next hop node of NHN. This cross checking loop will be continued until a trusted node is found. Moreover, in the case when the network in not under the attack, the algorithm takes more time to complete.

Agrawal[AGD08] etal. considers an ad hoc network with three type of nodes: low transmission range(RN) nodes, Backbone Nodes(BN) with higher transmission range, and Backbone Capable Nodes(BCN) which can be promoted to BN, to handle blackhole/grayhole attack . Initially a backbone network of BN nodes is established over the ad hoc network. The algorithm requires these BN nodes to monitor and detect the RN nodes if they act maliciously. With the assistance of the backbone nodes, the source and

the destination nodes carry out an end-to-end checking to determine whether the data packets have reached the destination or not. If the checking results in a failure then the BN nodes initiates a protocol for detecting the malicious nodes.

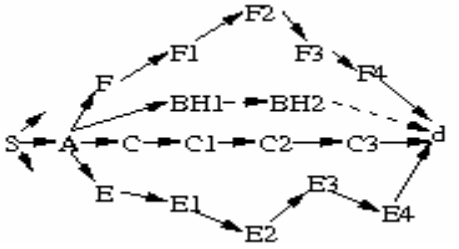
Bhargava et al. [BRYN09] proposes the idea of the three state model for handling the collaborative attacks. First state is monitoring state, where in network is observed for malicious activity. Using wavelet transform theory for monitoring state, it can be checked whether any deviation is there in the normal working of the network from the pre-defined behavior. Next state is characterization state. For characterization state, author proposes Fuzzy Logic concepts to determine best match for the deviation observed and the characteristics features of the type of attack. If the type of the attack is determined than the defense state is triggered. Where again the principles of Fuzzy Logic can be used to take remedial measures so that the effect of the single as well as multiple coordinated collaborative effect can be neutralized. In this paper, a collaborative model of attack among blackhole node (A) and Wormhole nodes (X, Y) as shown in below Figure is discussed. It is shown how against AODV routing protocol, using collaboration, collaborative malicious nodes can include itself into the path and can cripple the network.



Banerjee [] checks if the number of data packets dropped on a particular path is more than a tolerable threshold, it invokes the detection of blackhole/grayhole attack. For this it uses the neighbours of the nodes on the path to monitor whether a node is forwarding its data packets properly or not. However it is not clear what happens when a node colludes with its neigbhours to harbour an attack.

Proposed Work

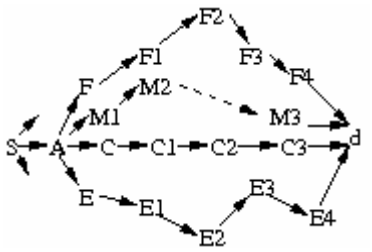
Modeling collaborative Black hole attack: Black node responds positively to a request for a shortest route, even though it does not have a valid route to the destination node.
Most of the algorithms to handle black hole attack (RAODV, Deng, Tamilselvan) perform cross-validation either with the NHN (next hop node) or with the destination. Consider the following model in which two or more malicious nodes collaborate to befool these solutions.



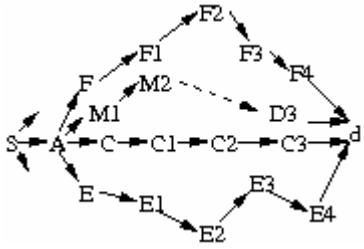
Suppose in the above figure a malicious node BH1 replies with a false route to the source. Let BH2 be another malicious node which is also the NHN of M1. When cross-validation is performed by say Deng, BH2 supports BH1 thereby defeating the algorithm, or when RAODV tries to check with the destination, if BH2 has a fresh route to the destination, BH1 uses BH2 to reach the destination and get the reply thereby again defeating the protocol.

Black nodes may also collaborate in sending multiple responses to request so that at least one of them gets included into path. The algorithm which collects multiple replies and uses strategy to pick one randomly may be prone to such type of attacks. Following figure depicts this model of collaboration amongst the black hole nodes.

Modeling collaborative Black hole and Wormhole attack: This type of collaboration may be more severe than collaboration among black nodes since in this wormhole nodes may be used to create a path from the blackhole node to the destination after M1 has replied to an RREQ to the source. This path may then be used to send the data packets to the destination but, the malicious nodes (M1,M2 or M3) can tamper the packets on its way or selectively drop the packets. The path through the wormhole tunnel can also be used to get any type of feedback or acknowledgement from the destination. Thus protocols like RAODV and PCBHA requiring cross-verification from the destination would fail in such a scenario. The one by Deng would certainly fail as M2 being the NHN of M1 would verify and support M1 in cross-validation.



Modeling collaborative Black hole and Rushing Attack: This model is similar to the above in which a blackhole node M1 replies to a route request without having a fresh route to the destination. Then, it establishes a path to the destination with the help of another malicious node M2 (causing rushing attack). This path can be used as above to befool various security protocols like RAODV,Deng and PCBHA.



Experiments

We propose to model collaborative attacks on routing protocols for ad hoc networks and devise solutions for them.

References

[BRYN09] Bharat Bhargava, Ruy de Oliveira1, Yu Zhang and Nwokedi C. Idika1 "Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks" IEEE International Conference on Distributed Computing Systems Workshops

[KG08] N. Gupta and S. Khurana. Seeep: Simple and efficient end-to-end protocol to secure ad hoc networks against wormhole attacks. In Proceedings of International Conference on Wireless and Mobile Communications, 2008.

[HPJ03] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings of INFOCOM, 2003.

[KBS05] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. Liteworp: A lightweight counter measure for the wormhole attack in multihop wireless networks. In Proceedings of International Conference on Dependable Systems and Networks (DSN), 2005.

[WBLW06] Weichao Wang, Bharat Bhargava, Yi Lu, and Xiaoxin Wu. Defending against wormhole attacks in mobile ad hoc networks. In Wiley Journal Wireless

Communications and Mobile Computing (WCMC), volume 6, pages 483 –503. Wiley, 2006.
[BB02] S. Buchegger and J.-Y. Le Boudec. Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). In Proceedings of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 226–236. Lausanne, Switzerland, ACM Press, 2002, 9-11 June, 2002.
[RFKN05] S. Ramaswamy, H. Fu, and K. Nygard, "Effect of Cooperative Black Hole Attack on Mobile Ad Hoc Networks," *Proc. ICWN*, Jun. 2005.
[AGD08] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.
[MGLB00] S**.** Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *6th MobiCom***,** Boston, Massachusetts, August 2000
[PM03] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks*," Proc. Radio and Wireless Conference RAWCON*, Aug. 2003.
[Map] Purdue University Wireless Mesh Network Testbed. https://engineering.purdue.edu/MESH.
[Deter] DETER: A Laboratory for Security Research, http://www.isi.edu/deter/.

[Emulab] Emulab - Network Emulation Testbed. ***http://www.emulab.net/***.