Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Implementation of Intrusion Tolerant Adhoc Routing in MANETS

MadhuKeerthi. T*
M.Tech 2nd year, Dept of CSE,
ASIT, GUDUR, India

P. Vindhya
Assistant Professor, Dept of CSE
ASIT, GUDUR, India

Abstract— In hostile environments, adversaries can launch passive attacks against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. In this paper we propose a feasible adversary model of such attacks, then present several instantiations and study the principles of designing corresponding countermeasures. We demonstrate that existing ad hoc routing protocols are vulnerable to passive attacks: in the feasible adversary model, (a) the location and motion patterns of mobile nodes can be traced, while (b) proactive and reactive/on-demand ad hoc routes across multiple mobile nodes can be visualized by the adversary. We conclude that ad hoc networks deployed in hostile environments need new countermeasures to resist such passive attacks.

Keyword terms: passive attacks, motion interface patternattacks,routing protocols

I. Introduction

Current military technology has already realized precise weapons to destroy distributed entities within several hundred feet at a time, while the area covered by a wireless hop in many ad hoc networking schemes is within this fatal range. Consequently, if the enemy is able to obtain definite(though imprecise) information about a VIP mobile node's location, then the specific target is exposed to great danger. Ad hoc networking can help legitimate nodes to establish an instant communication structure. Unfortunately, it may also allow passive adversaries to trace network routes and nodes at the end of those routes. Consider for example battlefield scenario with ad hoc, multi-hop wireless communications support. Suppose a covert mission is launched, which includes swarms of reconnaissance, surveillance, and attack task forces. The ad hoc network must provide routes between various task forces, and meanwhile hide their identities as well as motion patterns. It is clear that providing location privacy and motion privacy supports forth task forces is critical, else the entire mission may be compromised. This poses challenging constraints on secured hoc routing and data forwarding. it is necessary to address following problems to prevent the passive adversaries from tracing where a mobile node is, inferring the motion pattern of the mobile node, or visualizing a multi-hop path between any two legitimate nodes.

Defence against traffic analysis :

Traffic analysis is a network based attack against distributed systems. An external adversary needs *not* compromise a legitimate node or break relevant cryptographic designs, yet it can trace a packet flow using timing and other eavesdropped routing information. For example, in timing analysis, two packets transmitted in and out of inexplicit forwarding node at time t and t+_ are likely from the same packet flow.

Defence against passive internal adversary :

The electronic warfare in the two gulf war's demonstrates that the enemy's radars and other communication systems are facing immediate elimination once they are detected and targeted. Our likely enemies probably are not able to deploy a battle-ready mobile ad hocnetwork comparable to our armed forces. However, they may deploy passive attacking nodes like sensors. In addition, during a combat the enemies may be able to capture several legitimate ground nodes. To baffle our intrusion detection systems and followed countermeasures, it is appealing for them to use the captured nodes to launch passive attacks without introducing obvious anomalies into the network.

II. Related Work

2.1passive Adversary Model

Passive eavesdroppers may be omnipresent in a hostile environment where an ad hoc network is deployed. For example, nowadays technology has implemented wireless interface on low-cost sensor nodes (e.g., Motorola ColdFire,Berkeley Mote) which can in turn be planted in battlefields to monitor ongoing activities. It would be an impractical conjecture if we assume data packets transmitted in wireless broadcast channel are not to be intercepted by eavesdroppers. On the other hand, an adversary with unbounded cryptanalytic and intruding capability is capable of overwhelming any practical security protocol. Thus we study a powerful yet practical adversary with *unbounded* eavesdropping capability and *bounded* cryptanalysis and node intrusion capability:

Passive link intrusion capability:

An adversarial node at this level is an *external adversary* that poses threat to wireless link only. (1) The adversary knows and actualizes all network protocols and functions. It can eavesdrop and record wireless packets. (2) The adversary can access its computational resources via a fast network with negligible delay. This implies that collaborative adversaries can also contact each other in short latency. (3) However, their computational resources may be abundant, but not unbounded. They cannot break well-defined cryptosystems with nonnegligibleprobability

Passive node intrusion capability:

An adversarial node at this level is an *internal adversary* that also poses threat to network members. (1) After the adversary compromises a victim node, it can see the victim's currently stored records including the private route caches. (2) Intrusion detection is not perfect.

.

III. **PASSIVE ATTACKS AGAINST AD HOC ROUTING**

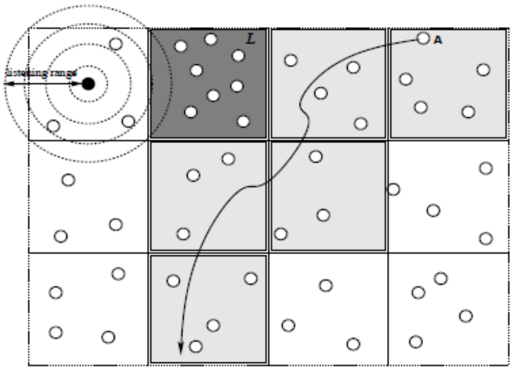

Fig. 1. **Passive traffic analysis: a referential scenario**

Fig. 1 shows the referential case for collaborative adversaries to trace the motion pattern of a mobile node. A collection of adversarial nodes can be (pre-)deployed to cover region or even the entire ad hoc network. As depicted in Figure 1, the adversaries can divide the network into cells based on radio receiving range. One or more adversarial nodes can effectively monitor each cell. Any open wireless transmission within one-hop transmission range is thus collected and fed back to adversary's computing centre for further analysis. The examples below demonstrate various passive attacks that can be launched by the adversaries. Encrypting lower-layer routing information seems to be a good solution to defend external adversaries. Basinet al. [2] propose a scheme to encrypt routing messages using a network-wide symmetric key shared by all legitimate members. However, the simple scheme has several drawbacks:

Simple encryption cannot completely stop traffic analysis, where external adversaries need *not* to break the encryption scheme as long as packet flows are forwarded without other protection. For example, if the encrypted payload is unchanged along a forwarding path, then external adversaries can simply do bit-string match on encrypted data to trace a flow. In addition, timing analysis is also a useful traffic analysis method to bypass cryptographic protections. Problems caused by passive internal adversary are not solved. Sharing a network-wide key is vulnerable to single intrusion of any legitimate node. Data encryptions a good solution to protect secret plaintexts, but does not necessarily offer protection when the secret key is revealed to internal adversaries. Then a node intrusion would ideally only compromise the transmissions related to the compromised keys cached by the victim.

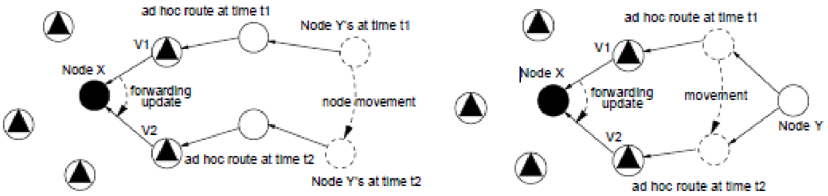

Fig. 2. **Motion pattern inference attacks** (left: target movement; right: forwarding node movement. Passive internal adversary is depicted as a solid black node in an H-clique)

We simulate a scenario where a target node moves sprightly across a network with many fixed nodes. While moving, the target node periodically communicates to other nodes. In the meantime, internal adversaries are presented in the network. In our simulation, we study two simple cases to illustrate the attack. In the first case, the target talks to one destination and there is only one adversary. In the second case, more adversaries exist in the networks, and the target talks to two destinations. Through the two cases, we demonstrated that with a certain number of adversaries(which are capable of communicating with each other), in bounded time, motion pattern inference is possible.

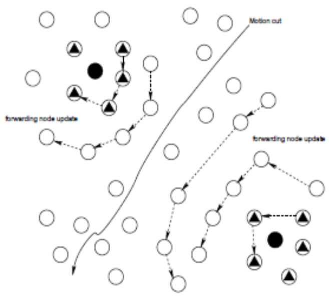

Fig. 3. **H-clique attack: a motion cutting through two H-cliques is detectable from forwarding node updates**

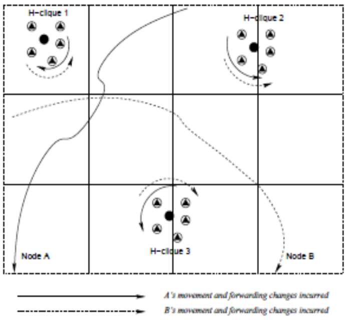
H-clique 1
H-clique 2
H-clique 3
Node A
Node B
A's movement and forwarding changes incurred
B's movement and forwarding changes incurred

Fig. 4. **Coalesceable H-clique attack: More H-cliques can obtain more precise motion patterns**

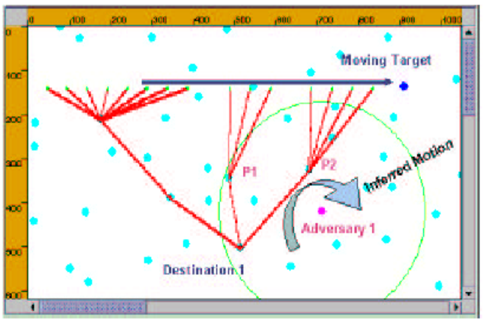

Fig. 5. **Illustration on actual simulation animation: Motion inference with one H-clique** (Depicted nodes and ad hoc routes are from actual GloMoSim animation)

In the simulation, we use AODV routing protocol to establish paths between the target and the destinations. AODV does not protect its routing information, thus any external adversary can also launch H-clique attack. As an on-demand protocol, AODV searches the destination when communication is needed. The search procedure starts by flooding a *Route Request (RREQ)* message for the destination. Upon receiving a request message, the destination will reply a *Route Reply (RREP)* message that traces the reverse path of the request back to the source, establishing apathy between the source and the destination. When the path breaks, e.g., a link broken due to mobility, the source willed-issue the search procedure to build a new path between the source and the destination.

Figures 5 and 6 are snapshots of our simulations. In the two figures, the target moves from the left of the simulation field to the right. A path between the target and the destination is depicted by linked solid lines. For each communication instance, the path in use is drawn in the figure. While the target is moving, different paths are chosen and the figure shows that the intermediate forwarding nodes have changed for several times in the simulation due to the target mobility. The adversary node and its radio range is also drawn in the figures. In Figure 5, node P1 and P2 are in the radio range of the adversary. During a certain time period, the adversary node hears the path change from P1 to P2 (it can do so either through AODV path setup messages or data packets). Thus the adversary infers that there is a clockwise motion to its north-west.

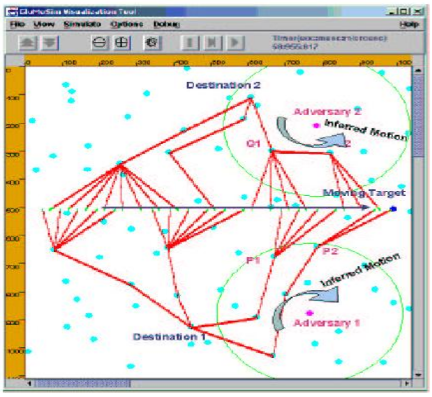

Fig. 6. **Illustration on actual simulation animation in GloMoSim: Motion-cut attack by 2 H-cliques** (Depicted nodes and ad hoc routes are from actual GloMoSim animation)

In Figure 6, the same target motion is detected by two adversaries. While the "adversary1" suggests clockwise motion to its north-west, the "adversary2",hearing the path migration from node Q1 to node Q2,figures out that the target is moving counter clockwise to its south-west. Combining these two pieces of information, the adversaries successfully discover that there is a motion cutting through between them. If more adversaries are presented in the network, more complete and precise motion pattern will be inferred.

IV DESIGN PRINCIPLES OF A ROUTING

Privacy in mobile networks have different semantics from the traditional ones for business banking. systems and the Internet. Cooper and Barman [5] identify three kinds of privacy for mobile computing: content, participant location, and participant identity. Content privacy can be easily ensured via traditional mechanisms using symmetric key and public key cryptosystems. To ensure privacy for mobile nodes' locations and identities, we must build new security mechanisms other than the ones used for content privacy.

Intrusion-tolerant ad hoc routing:

In hostile environments, intrusion is likely inevitable in a long time window. Proposal vulnerable to single point of compromise (e.g., centralized services) is not a proper solution. And a qualified solution should maximize its tolerance to multiple compromises, especially against passive internal adversaries who would exhibit no malicious behaviour and stay in the system. One-hop neighbour information must be hidden from these passive internal adversaries.

Robust against eavesdropper's traffic analysis:

Even if cryptographic schemes can ensure data privacy, networkbasedattack such as timing analysis can reveal the routing path according to temporal dependency in consecutive data forwarding. A qualified solution should ensure that timing analysis will be effectively stopped.

Fully dynamic routing information

Passive adversary can always use static routing information to trace legitimate nodes. To implement an anonymous and untraceable routing scheme, it is appealing to realize fully dynamic routing information. In the ideal case, any routing information issued once and only once, hence the adversary can obtain minimal information from such uniform distributions.

V. Conclusions

In this paper we propose a practical passive attack model against ad hoc routing protocols. We demonstrate that existing ad hoc routing protocols are vulnerable to the passive attacks. The work shows the necessity to devise untraceable ad hoc routing schemes to protect wireless nodes' mobile privacy in hostile environments. In addition to traditional content privacy concerns, mobile nodes need more support to ensure their location privacy, anonymity/identity privacy.

References

[1] C. Adjoin, T. Clausen, P. Jacque, A. Labourite, P. Pinetop. Muhlethaler, A. Qayyum, and L. Viennot. OptimizedLink State Routing Protocol. http://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-08.txt,March 2003.

[2] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi. Secure Pebblenets.In *MobiHoc*, pages 156–163, 2001.[3] M. Brown, D. Cheung, D. Hankerson, J. L. Hernandez, M. Kurkup,and A. Menezes. PGP in Constrained Wireless Devices. In *USENIXSecurity Symposium (Security '00)*, 2000.

[4] D. L. Chaum. Untraceable electronic mail, return addresses, anddigital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[5] D. A. Cooper and K. P. Birman. Preserving Privacy in a Networkof Mobile Computers. In *IEEE Symposium on Research in Securityand Privacy*, pages 26–38, 1995.

[6] B. Dahill, B. N. Levine, E. Royer, and C. Shields. A SecureRouting Protocol for Ad Hoc Networks. In *10th International Conference on Network Protocols (ICNP'02)*, 2002.

[7] Y.-C. Hu, D. B. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In *Fourth IEEE Workshop on Mobile Computing Systems*

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A Secure Ondemand Routing Protocol for Ad Hoc Networks. In *MOBICOM*, 2002.

[9] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in AdHoc Wireless Networks. In T. Imielinski and H. Korth, editors, *Mobile Computing*, volume 353, pages 153–181. Kluwer AcademicPublishers, 1996.

[10] J. Kong and X. Hong. ANODR: ANonymous On DemandRouting with Untraceable Routes for Mobile Ad-hoc Networks. In *MOBIHOC'03*, pages 291–302, 2003.

[11] R. Ogier, M. Lewis, and F. Templin. TopologyDissemination Based on Reverse-Path Forwarding (TBRPF).http://www.ietf.org/internet-drafts/draft-ietf-manet-tbrpf-07.txt, March 2003.

[12] C. E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *SIGCOMM*, pages 234–244, 1994.

[13] C. E. Perkins and E. M. Royer. Ad-Hoc On-Demand DistanceVector Routing. In *IEEE WMCSA'99*, pages 90–100, 1999.

[14] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLABroadcast Authentication Protocol. *RSA CryptoBytes*, 5(2):2–13, 2002.

[15] UCLA Parallel Computing Laboratory and Wireless Adaptive MobilityLaboratory. GloMoSim: A Scalable Simulation Environmentfor Wireless and Wired Network Systems. http://pcl.cs.ucla.edu/projects/glomosim/.