International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

Anonymous ALARAM to Withstand DoS Attacks

K.Ashokprabha [1], Durgaprasad Arigela[2], K.Srinivas[3]

1# PG Student, Department of CSE, BVC Engineering College,Odalarevu
2# Assistant Professor, Department of CSE, BVC Engineering College
3# Associate Professor, Department of CSE, BVC Engineering College

Abstract:

A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructure less, multi-hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: firstly, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; secondly, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; thirdly, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; The work mainly focuses on identifying preventive methods of impersonation security attacks on MANET

Index Terms—Privacy, communication system security, communication system routing, on-demand routing protocol, mobile communication, location-based communication, military communication.

Introduction

From literature study it is found that, Mobile Ad hoc Networks (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. A Mobile Ad hoc Network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Ad hoc Network usually seek the help of other intermediate nodes to establish communication channels. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. The security experience from the Wired Network world is of little use in wireless Mobile Ad hoc Networks, due to some basic differences between the two Networks. Therefore, some novel solutions are required to make Mobile Ad hoc Network secure.

A Mobile Ad hoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Application such as military exercises, disaster relief, and mine site operation may benefit from ad hoc networking, but secure and reliable communication is a necessary prerequisite for such applications MANETs are more vulnerable to attacks than wired networks due to pen medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered. Some of the weak points and solutions to strengthen them are considered.

Mobile Ad hoc Network(MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly exiles and robust.

Contributions: This paper makes two contributions. First, it shows how to obtain privacy-friendly on-demand location centric MANET routing. By “privacy-friendly” we mean *resistant to node tracking by both outsider and insider adversaries* Moreover, this is achieved without sacrificing security. Second, it demonstrates – via simulation – that the proposed PRISM protocol offers better privacy and better efficiency than prior results.

Challenges in Existing Systems

Adversarial model does not take into account adversaries that physically track nodes, e.g., visually or using physical-layer signal finger-printing. Furthermore, it does not consider adversaries that mount denial-of-service (DoS) attacks by creating sinkholes, wormholes and other topological abnormalities. We first discuss certain key features of the envisaged MANET setting and justify certain choices in our design. We present our assumptions and adversary model. We then describe the details of PRISM and analyze its security and privacy. PRISM's efficiency is compared through simulation to prior and an overview of related work is presented. work has three main goals:

(1) *Privacy:* maximize tracking-resistance of individual nodes, by outsider and insider adversaries.

(2) *Security:* provide protection against active and passive outsider and insider attacks.

(3) *Efficiency:* attain the above two goals with reasonably efficient solutions. The need for comprehensive addressing is fundamental in most networks. Some form of a unique address (or name) is usually a pre-requisite for one node to communicate with another. However, we argue that in a privacy-conscious MANET setting, using long-term or persistent identifiers can be harmful. The first threat comes from outsiders: tracking nodes based on their identifiers is possible by eavesdropping on routing information exchanged. This can be easily remedied by having all MANET nodes share a network-wide key and encrypting all routing information. The second threat comes from malicious insiders, i.e., MANET nodes that aim to track their peers. This threat is much harder to address, since a typical (even secure) MANET routing protocol is designed to provide routing information based on a destination address. *Network Assumptions*• A node has no public identity. There might be a private long-term identity (or address) for each node but this information is assumed to remain private between each node and a trusted off-line authority•

All communication is hit-and-miss and location-centric: A source node selects a destination location (area) and attempts to communicate to a destination node (or nodes) at that location. If the specified location is empty, the source node times out. Most communication sessions are short-lived.

The MANET environment is suspicious, meaning that even genuine nodes cannot be trusted.

• Each node has a means of determining its location with reasonable accuracy, e.g., a GPS device.

• Nodes are loosely time synchronized; (this feature is "free" with GPS).

- Nodes are capable of generating good-quality random numbers and performing basic public key operations (e.g., encryption and signatures).

Proposed Work

The main work of this paper is to address the security issue, because MANETs are generally more vulnerable and an extension of PRISM and ALARM protocol for MANETs, are named Heterogeneous ALARAM to Withstand DoS Attacks (H-ALARAM) based on AODV. This protocol is work on various modes; each mode corresponds to specific state of the node. This protocol is design to protect the network from malicious and selfish nodes. This project will use Extended Public key Cryptography mechanism in H-ALARAM in order to achieve security goals. AODV [5] presents an attractive foundation for PRISM, for several reasons. AODV is on-demand (reactive) and thus does not *propagate* topology information, in contrast with proactive protocols, such as OLSR. AODV is distance-vector; it does not return source routes (which reveal partial topology), unlike source-routing-based protocols, such as DSR. AODV is robust since it uses flooding for route discovery; thus, it does not require mobility to be synchronized. We do not describe AODV in detail, since, as an established routing protocol, it is well-known and has been extensively studied. Group signatures, described in [8], are an appealing building block for anonymous MANET routing protocols, mainly because they satisfy the conditional privacy property. Group signatures can be viewed as traditional public key signatures with additional privacy features. In a group signature scheme, any member of a large and dynamic group can sign a message, thereby producing a *group signature*. A group signature can be verified by anyone who has a copy of a constant-length group public key. PRISM is designed with the following features in mind: the source authenticates the destination and vice versa. Intermediate nodes do not learn current location of the source or the *exact* current location of the destination(s). Intermediate nodes are not authenticated. After route discovery, all communication between

TABLE 1
NOTATION USED

RREQ	Route Request
RREP	Route Reply
DST-AREA	Destination area
PKX, *SKX*	Public, private key of *X*
TSX	Time-stamp of *X*
GSIGX	Group signature generated by *X*
DSTLoc	Exact location of a destination node
H(*m*)	Hash of *m* (e.g., SHA-256)
EK(*m*)	Encryption of *m* with key *K*

source and destination is encrypted and authenticated using a one-time secret key. The TTP (group manager) can later learn claimed locations of all nodes that engage in direct communication, i.e., serve as either sources or destinations. The privacy achieved by PRISM is not restricted to a specific mobility pattern. The basic operation of PRISM is similar to AODV. PRISM allows a source to specify a destination area and simultaneously discover multiple destination nodes in it. However, to keep the description simple, we assume that only one node exists within each destination area. The source broadcasts a route request (RREQ) which contains the destination location, in the form of coordinates and a radius – DST-AREA. RREQ also contains a temporary public key *PKTMP*, a time-stamp *TSSRC* and a group signature, *GSIGSRC* computed over all previous fields. The RREQ message format upon receiving a RREQ, each node first checks if *TSSRC* is valid. If not, the RREQ is dropped. Next, the node checks whether it has previously processed the same RREQ. This is done by computing a hash of the new RREQ (*H*(*RREQ*)) and looking it up in the local cache where all recently handled RREQ hashes are stored. Upon receiving a RREP, each node checks whether it has cached the corresponding *H*(*RREQ*). If not, the RREP is dropped since this node was not on the forward route.

ALARAM RREQ Message

Message – Type PREQ (1 bytes)
DST – AREA (8 bytes)
PK_{TMP} (128 bytes)
TS_{SRC} (4 bytes)
$GSIG_{SRC}$(~200 bytes)

ALARAM RREP Message

Message – Type- RREP(1 byte)
H(RREQ) (32 bytes)
$E_{PKTIJP}(K_2)$(128 bytes)
E_{KS} (PST_{LDC}) (16 bytes)
$GSIG_{DST}$ (~200 bytes)

ALARAM Data Message Format

Message – Type- DATA(1 byte)

H(RREQ) (32 bytes)
H(RREP) (32 bytes)
TS_{SRC}(4 bytes)
E_{KS}(Data)

If *H*(*RREQ*) is already cached, the node checks if the same RREP has been processed. If so, the RREP is dropped. The intermediate node now creates a new entry in its active routes table and re-broadcasts the RREP. Each active table entry contains: *H*(*RREQ*), *H*(*RREP*) and the time-stamp of entry creation. When the RREP is received, the source first checks for the correctness of the time-stamp and the exact location of the replying node then verifies the group signature. If invalid, the RREP is discarded and logged as a failure. Next, the source decrypts the session key and location supplied by the destination. This key is subsequently used for message encryption and/or authentication. Next, the source stores the entire RREP for forensic purposes. This completes the route set-up process.

Conclusion

This paper presents the PRISM protocol which supports anonymous reactive routing in suspicious location-based MANETs. It relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. It works with any group signature scheme and any location-based forwarding mechanism. We evaluate its routing overhead and show that it can outperform anonymous link state based approaches under certain traffic patterns. We also evaluate PRISM's tracking-resistance by comparing its degree of topology exposure to link-state based approaches. PRISM reveals less of the topology and is thus more privacy-friendly.

References:

[1] B. Hartzog and T. Brown, “Wimax- potential commercial off-the-shelf solution for tactical mobile mesh communications,” *Milcom*, 2006.

[2] “RFC1677-Tactical Radio Frequency Communication Requirements for IPn,” http://www.faqs.org/rfcs/rfc1677.html.

[3] L. Kissner and D. Song, “Privacy-preserving set operations,” *CRYPTO*, 2005.

[4] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, “Enhancing wireless location privacy using silent period,” *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2, pp. 1187–1192 Vol. 2, March 2005.

[5] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90–100. [6] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, “Optimized link state routing protocol for ad hoc networks,” 2001, pp. 62–68. [Online]. Available: http://dx.doi.org/10. 1109/INMIC.2001.995315

[7] D. B. Johnson, D. A. Maltz, and J. Broch, “Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks,” in *In Ad Hoc Networking*. Addison-Wesley, 2001, pp. 139–172.

[8] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *roc. CCS 2004*. ACM Press, 2004, pp. 168–177.

[9] 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.

[10] S. Canard and M. Girault, “Implementing group signature schemes with smart cards,” in *CARDIS’02: Proc. 5th onference on Smart Card Research and Advanced Application Conference*. Berkeley,CA,USA: USENIX Association, 2002, pp. 1–1.

[11] K. El Defrawy and G. Tsudik, “Alarm: Anonymous location-aided routing in suspicious manets,” *IEEE ICNP 2007*, pp. 304–313, Oct. 2007.

[12]“Simpy simulator,” http://simpy.sourceforge.net/.

[13] “NumPy and SciPy packages,” http://numpy.scipy.org/.

[14] T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for ad hoc network research,” *Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, pp. 483–502, 2002.

[15] X. Hong, M. Gerla, G. Pei, and C. Chinag, “A group mobility model for ad hoc wireless networks,” *ACM/IEEE MSWiM*, 1999.

[16] W. jen Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, “Modeling time-variant user mobility in wireless mobile networks,” May 2007, pp. 758–766.

[17] N. S. Fan Bai and A. Helmy, “Important: A framework to systematically

analyze the impact of mobility on performance of routing protocols for adhoc networks,” in *INFOCOM*, 2003.

[18] Durgaprasad Arigela,

Assistant professor,

Department of Computer Science. BVC Engineering College, Odalarevu ”Heterogeneous alaram with stand Dos Attacks”, 2012.