International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 2 Issue 4 ǁ April. 2014 ǁ PP.10-13

An Unobservable Secure On-Demand Routing With D-Worm Detection In MANET

Ms.V.Dharani Meenakshi[1], Ms.P.Aileen Chris[2]
PG Scholar, Department of CSE, Karpagam University, Coimbatore, India
Assistant Professor, Department of CSE, Karpagam University, Coimbatore, India

Abstract— Mobile ad-hoc network (MANET) is a self-configuring infrastructure-less network of mobile devices. In wireless communication, the privacy-protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility. Many schemes have been proposed to protect privacy in ad hoc networks. In these schemes, data packets and control packets are not completely unlikable and unobservable, and it will be distinguishable by harm users. An unobservable secure on-demand routing (USOR) protocol provides complete unlinkability and content unobservability for all type of packets using group signature and ID-based encryption. USOR Protocol did not see any worm in the content particularly disguising worm. The proposed scheme is detecting disguised worm using spectrum based scheme. This scheme uses power spectral density and spectral flatness measure. Spectrum based method not only detect disguising worm, but traditional worms as well**.**

Keywords—USOR, Anonymity, Unobservability, Unlinkability.

I. INTRODUCTION

MANET is a mobile wireless network, capable of autonomous operation & it operates without base station infrastructure. Privacy protection of mobile ad-hoc networks is more demanding than that of wired networks. In wireless network, attacker only need an appropriate transceiver to receive signal without detected. Hence in wireless network, privacy preserving is needed not only for the content of the message but also for its mobility behavior. Unobservable Secure On-Demand Routing (USOR) Protocol is used for secure routing and data transmission along with detecting malicious node to avoid node compromising using spectrum based method. USOR Protocol provides complete unlinkability and content unobservability to provide secure routing in Mobile Ad-Hoc Network. To achieve this uses a novel combination of anonymous key establishment from group signature signing key for content unobservability and ID-based private key for encryption to secure data transmission. Instead of using physical address as MAC address, they set their network interfaces in the promiscuous mode to receive all the MAC frames that can be detected in the neighborhood. This is important to prevent traffic analysis based on MAC addresses. Disguising worm is detected in the frequency domain. Measuring bandwidth for intrusion detection but it is like violation of people's privacy. Hence, instead measuring bandwidth between two nodes, it is measured with aggregated data using grid technology

A. PRIVACY PRESERVING PROPERTIES

Privacy-Preserving is known as maintaining the private information securely. To achieve secure routing and data transmission USOR achieve below properties

- Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.
- Unlinkability of two or more IOI from an attacker's perspective means that the attacker cannot sufficiently distinguish whether the IOI□s are related or not from the attacker's view.
- Unobservability of IOI from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not is indistinguishable to all unrelated subjects,and subjects related to this IOI are anonymous to all other related subjects

II. SCOPE

EXISITING SYSTEM

Existing system fail to protect all content of packets from attackers since protocols mainly consider anonymity and partial unlinkability. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection. so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which breaks unlinkability and may lead to source trace back attacks and make existing schemes observable to the adversary

PROPOSED SYSTEM

The proposed system each node can establish a key with each of its neighbors and that key to encrypt the whole packet for a corresponding neighbor hence protect all parts of a packet's content i.e., packet header is hided. To achieve unobservability, anonymous key established between neighbor for secure routing and so adversaries can't identify nodes involved in transmission and traffic information is hided by using network interface in promiscuous mode instead to physical address

SYSTEM ARCHITECTURE

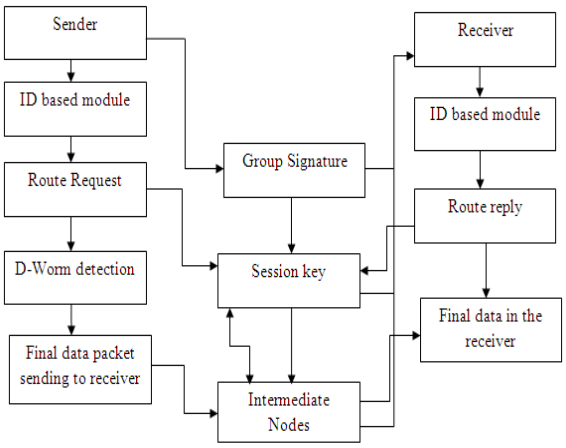


Fig.1 System Architecture

Each node involve in transmission establish anonymous key for group signature with its neighbors and ID based encryption key for secure data transmission. To establish routing, sender broadcast its signature message to all its neighbor, for acquire anonymous key to its neighbor without reveals its own identity. Sender broadcast route request message by encrypt using anonymous session key which only decrypt by appropriate receiver. Route reply message is unicast to sender using same anonymous session key. Depending upon least number of hops, data transmission is done by encrypting using ID-based key. Based on aggregated bandwidth measurement D-worm is detected. Encryption is made between intermediate node

A. ***Abbreviations and Acronyms***

A	A node in the ad hoc network, and its real identity
s	The master secret key owned by the key server
q	A 170-bit prime number
P	Generator of the elliptic curve group G1
Hi(∗)	Secure one-way hash functions, *i* = 1, 2, 3 †
gskA	Node *A*'s private group signature key
gpk	The public group signature verification key
KA	Node *A*'s private ID-based key which is $s \cdot H1(A)$
EA(∗)	ID-based encryption using *A*'s public key
$\bar{}kA*$	A local broadcast key within *A*'s neighborhood
kAX	A pairwise session key shared between *A* and *X*
Nym*A*	The pseudonym only valid within *A*'s neighborhood
Nym*AX*	The pseudonym shared between *A* and *X*

B. Anonymous Key Establishment

Each node that can communicate with its neighbor in its range. If a node S , then it has the private signing key *gskS* and a private ID-based key *KS* . The procedure for anonymous key establishment is follows.

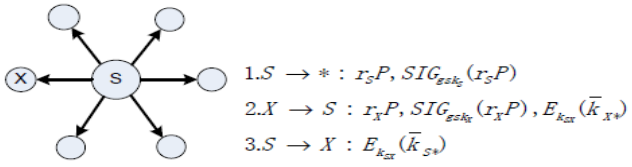


Fig.2 Anonymous Key Establishment

(1) *S* generates a random number $rS \in Z*q$ and computes *rSP*, where *P* is the generator of G1. It then computes a signature of *rSP* using its private signing key *gskS* to obtain *SIGgskS* (*rSP*). Anyone can verify this signature using the group public key *gpk*. It broadcast *_rSP, SIGgskS* (*rSP*)_ within its neighborhood.

(2) A neighbor *X* of *S* receives the message from *S* and verifies the signature in that message. If the verification is successful, *X* chooses a random number $rX \in Z*q$ and computes *rXP*. *X* also computes a signature *SIGgskX* (*rSP*|*rXP*) using its own signing key *gskX*. *X* computes the session key *kSX* = *H*2(*rSrXP*), and replies to *S* with message *_rXP, SIGgskX* (*rSP*|*rXP*),*EkSX* ($\bar{}kX*$ |*rSP*|*rXP*)_, where $\bar{}kX*$ is *X*'s local broadcast key.

(3) Upon receiving the reply from *X*, *S* verifies the signature inside the message. If the signature is valid, *S* proceeds to compute the session key between *X* and itself as *kSX* = *H*2(*rSrXP*). *S* also generates a local broadcast key $\bar{}kS*$, and sends *EkSX* ($\bar{}kS*$ |$\bar{}kX*$ |*rSP*|*rXP*) to its neighbor *X* to inform *X* about the established local broadcast key.

(4) *X* receives the message from *S* and computes the same session key as *kSX* = *H*2(*rSrXP*). It then decrypts the message to get the local broadcast key $\bar{}kS*$.

C . Privacy Preserving route discovery

This phase is based on the keys established in the previous phase & it encloses the route request & route reply. The route request messages that overflows in entire network. The route reply is sent to source node only.

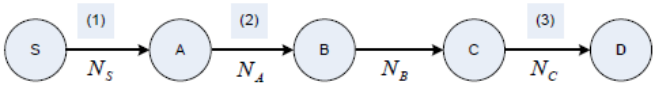
Consider source node as S, destination node as D then S has to find a route to D. Let as assume there three intermediary nodes between S & D.

Route Request

S chooses a random number *rS*, and uses the identity of node *D* to encrypt a trapdoor information that only can be opened with *D*'s private IDbased key, which yields *ED*(*S,D, rSP*). *S* then selects a sequence number *seqno* for this route request, and another random number *NS* as the route pseudonym, which is used as the index to a specific route entry. To achieve unobservability,

S chooses a nonce *NonceS* and calculates a pseudonym as

Nym*S* = *H*3($\bar{}kS*$ |*NonceS*).



(1) : $Nonce_S, Nym_S, E_{\bar{k}_{S*}}(RREQ, N_S, E_D(S, D, r_SP), seqno)$

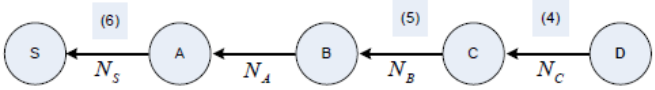
(2) : $Nonce_A, Nym_A, E_{\bar{k}_{A*}}(RREQ, N_A, E_D(S, D, r_SP), seqno)$

(3) : $Nonce_C, Nym_C, E_{\bar{k}_{C*}}(RREQ, N_C, E_D(S, D, r_SP), seqno)$

Fig.3 Route Request

Route Reply

After node *D* finds out he is the destination node, he starts to prepare a reply message to the source node. For route reply messages, unicast instead of broadcast is used to save communication cost. *D* chooses a random number *rD* and computes a ciphertext *ES*(*D, S, rSP, rDP*) showing that he is the valid destination capable of opening the trapdoor information. A session key *kSD* = *H*2(*rSrDP*|*S*|*D*) is computed for data protection. Then he generates a new pairwise pseudonym Nym*CD* = *H*3(*kCD*|*NonceD*) between *C* and him



(4) : $Nonce_D, Nym_{CD}, E_{k_{CD}}(RREP, N_C, E_S(D, S, r_SP, r_DP), seqno)$

(5) : $Nonce_C, Nym_{BC}, E_{k_{BC}}(RREP, N_B, E_S(D, S, r_SP, r_DP), seqno)$

(6) : $Nonce_A, Nym_{SA}, E_{k_{SA}}(RREP, N_S, E_S(D, S, r_SP, r_DP), seqno)$

Fig. 4 Route Reply

D. UNOBSERVABLE DATA TRANSMISSION

After thesource node *S* successfully finds out a route to the destination node *D*, *S* can start unobservable data transmission under the protection of pseudonyms and keys.

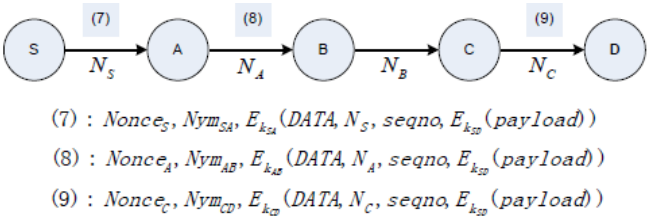


Fig.5 Data Transmission

E. Detecting the disguising worm

Even the complete message is unobservable using USOR, malicious node may present between routing which may involves in route compromising in order to obtain valid network information. An extension of onion routing with dynamic token exchange has been used for protecting from intruders. Detecting D-worm based on spectral based method is by measuring bandwidth not between the two nodes but message from bandwidth from all its neighbor of certain node

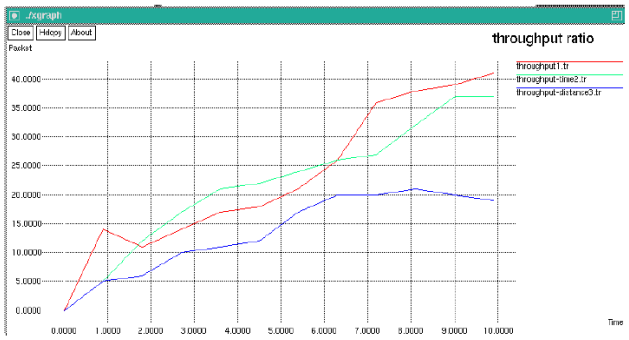


Fig.6 Throughput ratio Graph

III. Conclusion

Here, an unobservable secure on-demand routing protocol based on group signature and ID-based cryptosystem for ad- hoc networks is designed, and developed. The design of USOR offers strong privacy protection and unlinkability and content unobservability for ad-hoc networks but not detect D-worm. In a proposed work, a spectrum based detection scheme to detect disguising worm based on power spectral density and spectral flatness measure. Spectrum-based scheme detection is not only detecting the D-worm, but traditional worms as well.

REFERENCES

[1] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

[2] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in *PET04, LNCS 3424*, 2004, pp. 207–225.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. of the ACM*, vol. 4, no. 2, Feb. 1981.

[4] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.

[5] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *Proc. ACM MOBIHOC' 03*, pp. 291–302.

[6] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in *Proc. 2004 IEEE Conference on Local Computer Networks*, pp. 102–108.

[7] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in *Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications*, pp. 133–137.

[8] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in *Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 33–42.