Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Unidentified Position-Based Capable Routing Protocol in Mobile Adhoc Networks

Vinodh Kumar. K[*]
Research Scholar
Department of Information Technology
St Peter's University
Tamil Nadu, India

Dr. S. PadmaPriya
Professor & Head
Department of Information Technology
Prathysha Institute of Technology and Management
Tamil Nadu, India

Abstract*— Attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale. DDoS attacks usually involve early stage actions such as multistep exploitation, low-frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. To prevent vulnerable virtual machines from being compromised in the cloud, a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE is been proposed, which is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. The proposed framework leverages Open flow network programming APIs to build a monitor and control plane over distributed programmable virtual switches to significantly improve attack detection and mitigate attack consequences.

***Keywords*— Cloud, DDos, IaaS, NICE, Open flow Network, API.**

I. INTRODUCTION

RAPID development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyse data and traffic analysis by communication eavesdropping or attacking routing protocols.

Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage.

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. "Identity and location anonymity of sources and destinations" means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations.

For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic, Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned Anonymity protections.

II. PROBLEM STATEMENT & DEFINITION:

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy costto precious resource because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity

ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility mode.. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide untraceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field.

III. LITERATURE REVIEW

1.An Efficient Secure Route Discovery Protocol for DSR- Kulasekaran A. Sivakumar and Mahalingam Ramkumar Department of Computer Science and Engineering Mississippi State University ,MS. Nov 30,2007.

Ensuring cryptographic integrity of the route discovery process in on demand ad hoc routing approaches like DSR require the ability to verify that no nodes have been deleted from the path, and no node can be inserted in the path without a valid authentication. We discuss the need for early detection of inconsistencies involving inserted or deleted nodes in route request (RREQ) packets and investigate the challenges associated with catering for this requirement.

We propose an efficient strategy to achieve these employing only symmetric cryptographic primitives, which is made possible due to a recently proposed multi-source broadcast encryption scheme. We outline a protocol for secure route discovery in DSR that employs such a security primitive, and provide quantitative estimates (through simulations) of gains that can be achieved by early detection of inconsistent RREQs.

2. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs Karim El Defrawy and GeneTsudikSchool of Information and Computer Science University of California ,Sep 2011.

In many traditional mobile network scenarios, nodes establish communication on the basis of persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. Instead, nodes need to communicate on the basis of nothing more than their current locations.

In this Project ,we address some interesting issues arising in such MANETs by designing an anonymous routing framework (ALARM). It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and intractability (tracking-resistance). It also offers resistance to certain insider attacks.

3. Untraceability of Group Signature Schemes based on Bilinear Mapping and Their Improvement Haeryong Park ; Cryptography Technol. Team, Korea Inf. Security Agency, Seoul ; Hyun Kim ;Kilsoo Chun ; Jaeil Lee ,April 2007.

We propose a new group signature scheme which is secure if we assume the Decision Diffie-Hellman assumption, the *q*-Strong Diffie-Hellman assumption, and the existence of random oracles. The proposed scheme is the most efficient among the all previous group signature schemes in signature length and in computational complexity. This encryption scheme is more complex than the ordinary ElGamal type encryption scheme. The scheme also realizes a special authority that can identify actual signers in case of dispute. Group signatures have many applications in which user anonymity is required such as in anonymous credential systems, identity escrow, voting and bidding, and electronic cash systems.

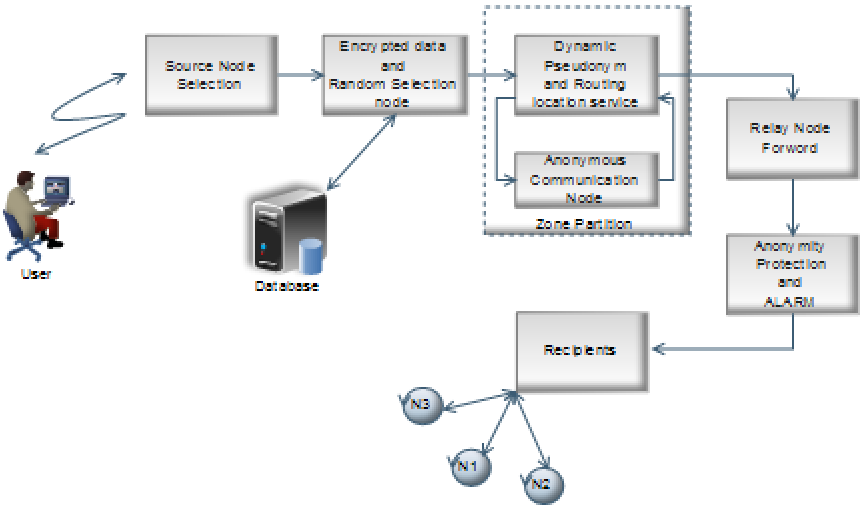
4. Location updates for efficient routing in ad hoc networks Ivan Stomenovic Computer Science, SITE, University of Ottawa, Ottawa, Ontario K1N 6N5, Canada, April 2008.

This chapter reviews research on routing in ad hoc and sensor wireless networks in the view of node mobility, changes in node activity, and availability of methods to determine absolute or relative coordinates of each node. Various approaches in literature are classified according to some criteria. Mobility is apparently a very difficult problem to handle in ad hoc networks, and all proposed solutions have significant drawbacks. Additional problems arise with 'sleep' period operation, that is changes in node's activity status with or without mobility. While significant progress has been made on the routing with known destination location, location updates issue to enable efficient routing requires further investigation.

5. S.Padma Priya, Dr. Jayaram Pradhan, "An Efficient security framework for detection and isolation of attacks in low rate wireless PAN , IJCSNS , Korea 2008, Vol. 8 No. 7 pp. 224-232" -

LR-WPANs pose a number of new security problems in addition to the problems of regular networks. Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. Packet delivery in adhoc networks is achieved through routing and packet forwarding. So we should provide security for both operations. We provide an Efficient Security Framework (ESF) that protects both routing and data forwarding operations. Our framework involves (i) Detection of malicious nodes by the modified AODV protocol. (ii) Isolation of malicious nodes by using Multi-Signature based tickets. Through both analysis and simulation results, we demonstrate the effectiveness of our framework in a highly mobile and hostile environment.

III. SYSTEM ARCHITECTURE


Source Node Selection
Encry pted data and Random Selection node
Dynamic Pseudony m and Routing location service
Anonymous Communication Node
Zone Partition
Relay Node Forword
Anony mity Protection and ALARM
Recipients
User
Database
N3
N1
N2

The user selects the source node from the no of nodes in a random way. After the node has been selected it should be encrypted and stored in a database. Now the encrypted node is moved into zone partition. Zone Partition It is the intercommunication between the anonymous communication node and Dynamic Pseudonym. Now the node information is passed into the Relay node through Routing location service. The received node is in the secured process and it is preceded to the recipient through the ALARM after it has been passed from anonymity protection. Now the final recipients will be in the types of nodes.

IV. SYSTEM IMPLEMENTATION

Several models that are implemented based on above techniques are as follows:

ALERT is compared with two recently proposed anonymous geographic routing protocols: AO2P and ALARM which are based on hop-by-hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare ALERT with the baseline routing protocol GPSR in the experiments. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination. In ALARM, each node periodically disseminates its own identity to its authenticated neighbors and continuously collects all other nodes' identities. Thus, nodes can build a secure map of other nodes for geographical routing. In routing, each node encrypts the packet by its key which is verified by the next hop en route. Such dissemination period was set to 30 s in this experiment. The routing of AO2P is similar to GPSR except it has a contention phase in which the neighbouring nodes of the current packet holder will contend to be the next hop. This contention phase is to classify nodes based on their distance from the destination node, and select a node in the class that is closest to destination

4.1 ZONE PARTITION

It is this Process network can be divide into set of zones. In this zone can communicate the different zone in the network. Increased a network weight's mean to automatically assign a Zonal partition by equal dividends

4.2 SOURCE NODE ENCRYPTION AND RANDOM FORWARD SELECTION

The source node protection and encryption the data's from source side. Then random forwarder can choose the randomly in the node. Then verify a node status and transmit data to the network. Source Node Encryption techniques which is divide the node and formed as in several parts sorted and framed as new node and its act as a normal node.

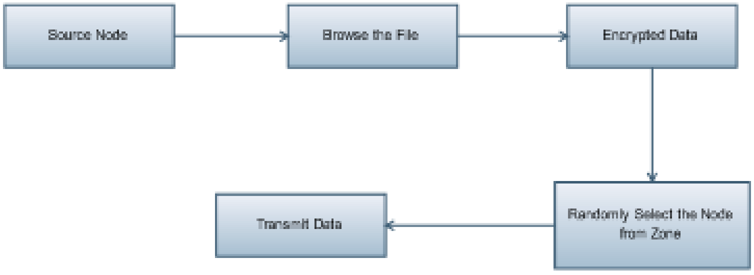


Fig 4.2 Source node encryption and random forward selection

4.3 RELAY NODE SELECTION

The relay node forwarded the next zone in the network. This can forward the data. It acts as an intermediate transaction in one zone to another zone. A network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no traceable anonymous route.

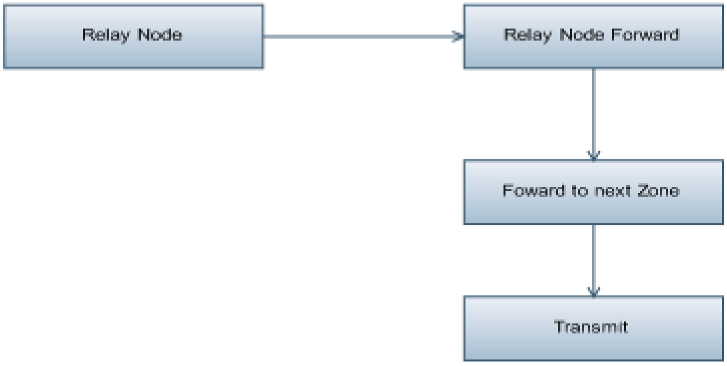


Fig 4.3 Relay node selection

4.4 ROUTING TABLE:

The routing table can update the routing path. It can attach the time stamp. The routing table frequently changed. Because routing table is finding the path hop-by –hop communication based

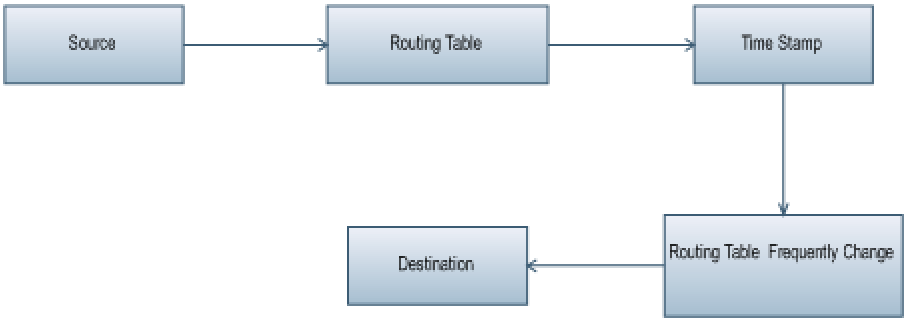


Fig 4.4 Routing table

4.5 DESTINATION NODE DECRYPTION AND VERIFICATION

Destination node received the data's from the network. To analyse the packet status (in case of any damage through the communication). Destination Node Decryption techniques which is reassembly the Node and its framed as new node. Decrypt a data to verify the original messages.

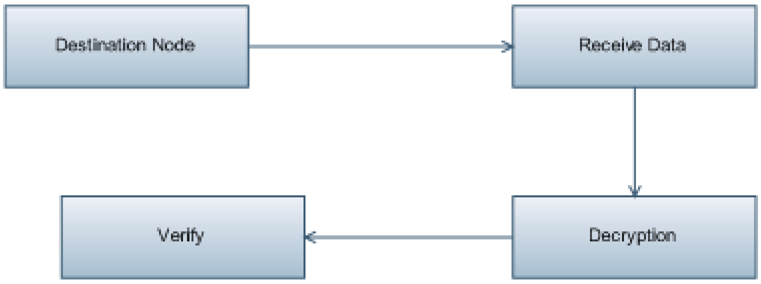


Fig 4.5 Destination node decryption and verification

V. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed.

REFERENCES

[1] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[2] Kulasekaran A. Sivakumar and Mahalingam Ramkumar Department of Computer Science and Engineering Mississippi State University,MS. "An Efficient Secure Route Discovery Protocol for DSR" Nov 30,2007.

[3] Karim El Defrawy and Gene Tsudik School of Information and Computer Science University of California "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs"Sep 2011.

[4] X. Wu, J. Liu, X. Hong, and E. Bertino, “Anonymous Geo- Forwarding in MANETs through Location Cloaking,” IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct.2008. Debian Administration.

[5] Haeryong Park ; Cryptography Technol. Team, Korea Inf. Security Agency, Seoul ; Hyun Kim ;Kilsoo Chun ; Jaeil Lee “Untraceability of Group Signature Schemes based on Bilinear Mapping and Their Improvement”April 2007.

[6] Srdjan Cˇ apkun, LeventeButtya, and Jean-Pierre Hubaux Laboratory for Computer Communications and Applications (LCA) School of Information and Communication Sciences (I&C) “Self-Organized Public-Key Management for Mobile Ad Hoc Network”

[7] S.Padma Priya, Dr. Jayaram Pradhan, “An Efficient security framework for detection and isolation of attacks in low rate wireless PAN , IJCSNS , Korea 2008, Vol. 8 No. 7 pp. 224-232”