International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP216-222

Unobservable Secure on Demand Routing Protocol (USOR) to Avoid Eavesdropping Attack

Rajani Patil[1], Prof. Dhanashree Kulkarni[2]
[1]*Department of Computer Engineering ,Dr. D.Y. Patil College of Engineering, Ambi, Pune University*
[2]*Department of Computer Engineering ,Dr. D.Y. Patil College of Engineering, Ambi, Pune University*

Abstract :- Wireless ad hoc network is self-directed and infrastructure less network. Wireless ad hoc network is particularly inclined due to its basic characteristics, such as open medium, dynamic topology, distributed cooperation, and capability constraint. Routing plays an important role in the security of the entire network. Secure transmission of information in wireless adhoc environment is an important concern. Any attacker receive wireless signal by using transceiver and without being detected. The objective of this paper is to propose new secure unobservable routing protocol where attacker gets blocked while making spoofing or DOS attacks. Only unobservant message could be collected by attacker. Proposed protocols also protect privacy information among network and detect and block attacking nodes through trust mechanism.

Keywords: - DOS attack, spoofing, Sensor networks, secure unobservable routing protocol

INTRODUCTION

A wireless adhoc network is collection of thousands of tiny wireless sensor nodes for data communication purpose. These sensor nodes cooperate with each other to accomplish data transmission. Numerous applications built in WSN like security, inventory tracking, automotive control, surveillance, health monitoring and other civil tasks, bridge monitoring, and home automation in the recent years. Sensors are inexpensive, low power devices, which have limited resources.

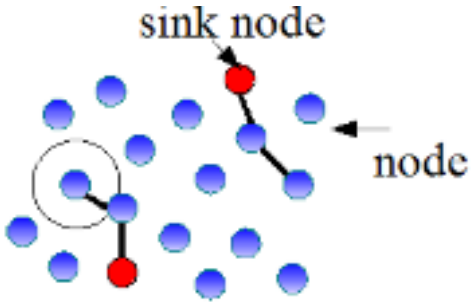

Fig 1: WSN Architecture

Fig.1 shows system architecture of wireless sensor network. The number of sensor node in WSN are usually large. Each node contains a power unit, processing units, a storage units, sensing unit and wireless transmitter or receiver. The Sensor nodes communicate with each other through simultaneous transmission of data from one node to another node. As transmitter range is limited, data must be forwarded in multiple hosts in order to reach remote node which is at long distance from originating source node. Cost of sensor node depends on complexity of applications. The sensors are still available at low cost. Generally, star topology is used in WSN.

Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks, one can start eavesdropping after getting access to wired cables. In contrast, in WSN, the attacker only needs an appropriate transceiver to receive wireless signal without being detected. In wired networks, devices like desktops are always static and do not move from one place to another. Hence in wired networks there is no need to protect user's mobility behaviour,

while this sensitive information should be kept private from adversaries in wireless environments. Otherwise, an adversary able to profile users according to their behaviours, and endanger or harm users based on such information. Providing privacy protection for ad hoc networks with low-power wireless devices and low bandwidth network connection is very challenging task.

II . SECURITY REQUIREMENTS IN WSN

WSNs are special kind of Ad-hoc networks. Security services in WSNs are required to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

Availability [11]: Availability ensures that the desired network services are available even in the presence of denial-of-service attacks.

Authorization: Authorization [11] ensures that only authorized sensors can be involved in providing information to network services.

Privacy: Privacy prevents adversaries from obtaining information that may have private content.

Authentication [6]: which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.

Anonymity: Anonymity [1][6] hides the source of the data. It is a service that can help with data confidentiality and privacy.

Unlinkability: Unlinkability[1][6] of two or more Item of identity (IOI) means these IOIs are no more or no less related from the assailant's perspective.

Unobservability: Unoservability[1][6] of IOI express that whether it exists or not is undefined to all random subjects, and subjects identified with this IOI are nameless to all other related subjects. It is of two types :

Content Unobservability[6], referring to no useful information can be extracted from content of any message

Traffic Pattern Unobservability[6], referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

Resilience [11]: Resilience sustains the network functionalities when a portion of nodes are compromised by the attacks.

Confidentiality [11]: Confidentiality ensures that a given message cannot be understood by anyone other than the desired recipients.

Integrity [11]: Integrity ensures that a message is not modified during the transmission.

Nonrepudiation [11]: Nonrepudiation denotes that a node cannot deny sending a message, it has previously sent.

Secure Localization [11]: In WSN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault.

Freshness: Freshness implies that the data is recent and ensures that no adversary can replay old messages. To make sure that no old messages replayed,a timestamp can be added to the packet. Sensor nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSN.

III. SECURITY THREATS AND ATTACKS IN WSN

[1] Denial Of Service: The DOS attack [6] tries to busy the available resource by the victim node by sending extra unnecessary packets result is other network users cant uses the available resources. DOS attacks disrupt the network as well as block the services. Strong authentication and identification is required for Prevention from the DOS attack.

[2] Attack on information in transit: The information during transit may be changed, spoofed, replayed again. This node provides incorrect information to sink node.

[3] Sybil attack [6]: In WSN Sensor nodes are works together for completion of any task. Sensor nodes divide their task into subtasks and redundancy of information. In this condition node can represent to be more than one node is known as Sybil attack.

[4] Blackhole attack [6]: In this type of attack a malicious node represent as black hole to induce all the traffic in the sensor network. Once malicious node introduced into the network, then it able to do anything with packet passing between them.

[5] Wormhole attack [6]: Wormhole attack is one of the critical attacks. In this type of attack attacker records the packet coming from one location and underpass those to another location. In this attack no need to compromising a sensor node.

[6] Gray hole [6]: Gray hole is a node that selectively omits packet with certain probability causing network distraction. Gray hole may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. In another way, gray hole may also behave maliciously for some time period by dropping all packets but may switch to normal behavior after some time. A gray hole may also illustrate a behavior having combination of the above two.

[7] Jellyfish attack [6]: In jellyfish attack, the malicious node first intrudes into the forwarding group in the network and then it unreasonably delays data packets for some amount of time before forwarding them. This result in significantly high end to- end delay and delay jitter, and thus degrades the performance of real-time applications.

[8] Spoofing [6]: This occurs when a malicious node pretends to be identity of other nodes. This will misguides a non-malicious node in order to change the vision of the network topology that it can gather.

IV. LITERATURE SURVEY

ALARM: ANONYMOUS LOCATION-AIDED ROUTING IN MANET [10]

ALARM [10] uses nodes' present areas to safely scatter and build topology snapshots and forward information. With the help of advanced cryptographic strategies, ALARM [10] provides both security and protection peculiarities, including node authentication, data integrity, anonymity, and un-traceability. It offers security against passive and active insider and outcast assaults. To the best of our insight, this work speaks to the first thorough investigation of security, protection, and execution trade-offs in the context of link-state MANET routing.

ANODR, ANONYMOUS ON-DEMAND ROUTING PROTOCOL [8]

ANODR [8], an anonymous on-demand routing protocol for mobile ad hoc networks deployed in unpredictable environments. In hostile situations, permitting attackers to follow network paths and nodes toward the end of those paths may posture genuine dangers to the achievement of covert missions. By using ANODR adversaries cannot discover the real identities of local transmitters. The design of ANODR [8] is relying on “broadcast with trapdoor information” ANODR[8] dissociates ad hoc routing from the design of network member’s identity. The adversary unable to link network members’ identities with their locations, also do not follow a packet flow to its

source and destination ANODR[8] ensures there is no single point of failure in ad hoc routing. Node invasion does not compromise location privacy of other genuine members, and an on-demand ANODR [8] route is traceable only if all forwarding nodes enroute are intruded.

.

SELF-ORGANIZED PUBLIC KEY MANAGEMENT FOR MANET [2]

In contrast with conventional networks, mobile ad hoc networks usually do not provide online access to trusted authorities or to centralized servers, and they exhibit frequent partitioning due to link and node failures and to node mobility. For these reasons, traditional security solutions that require online trusted authorities or certificate repositories are not well-suited for securing ad hoc networks. The fully self-organized public-key management [2] system allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, this approach does not require any trusted authority, not even in the system initialization phase.

ON FLOW CORRECTION ATTACKS AND COUNTERMEASURES IN MIX NETWORKS [3]

In this paper, issues related to flow correlation attacks and the corresponding countermeasures in mix networks are taken into consideration. Mixes have been used in many anonymous communication systems and are supposed to provide countermeasures that can defeat various traffic analysis attacks. This paper focus on a particular class of traffic analysis attack, flow correlation attacks [3], by which an adversary attempts to analyze the network traffic and correlate the traffic of a flow over an input link at a mix with that over an output link of the same mix. Two classes of correlation methods are considered, namely time-domain methods and frequency-domain methods. The empirical results give an indication to designers of mix networks about appropriate configurations and alternative mechanisms to be used to counter flow correlation attacks.

V. PROPOSED SCHEME

The proposed scheme is consisting of procedure to develop a new secure routing protocol where attacker got blocked while making spoofing or DOS attacks [6]. We covered following key objectives,

Sender, intermediate and destination node cannot identified by network

Link information also protected

Only unobservant message could be collected by attacker

Node can compromise easily by attacks is protected by privacy preserving routing protocol, Our protocol should protect privacy information among network

To detect and block attacking nodes through trust mechanism.

UNOBSERVABLE ROUTING SCHEME

we present an efficient unobservable routing scheme USOR[6] for ad hoc networks. In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pairwise key are needed.

As a result, USOR comprises three phases as follows :

[9] Key Generation

[10] Group Signature Scheme.

[11] ID-based Encryption Scheme.

[12] Anonymous Trust Establishment

[13] Unobservable Route Discovery

[14] Route Request.

[15] Route Reply.

[16] Attack Analysis.

[17] Data Transmission.

VI. OVERALL SYSTEM ARCHITECTURE

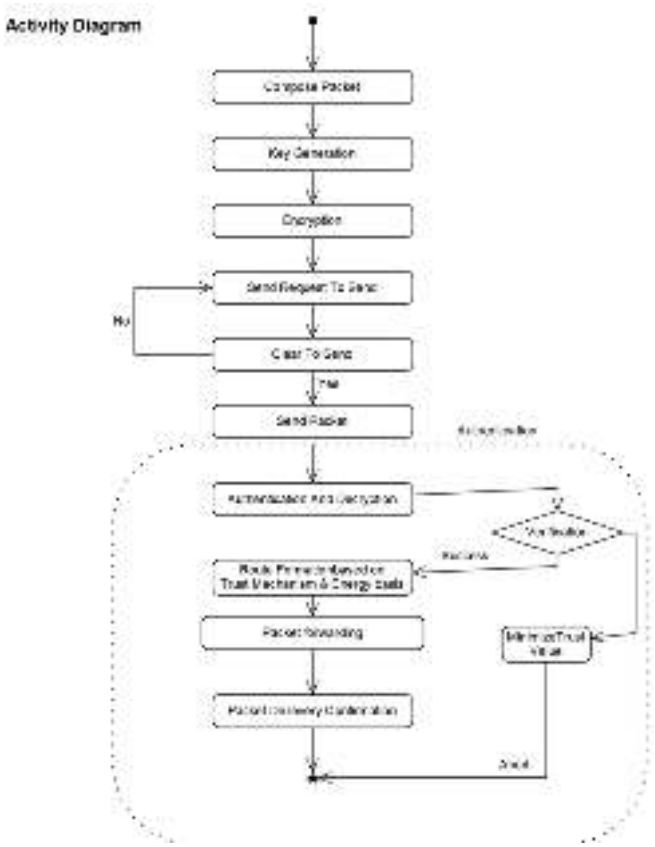

Fig 2 : USOR System Architecture

VII. COMPARATIVE ANALYIS

TABLE 1: Comparison

Protocol	Unobervability	Unlikability	Anonymity	Attacks Detected
USOR	Yes	Yes	Yes	Malicious node attack
ANODR	No	No	Yes	Location privacy attack, Route tracing attack
AnonDSR	No	No	Yes	Does not deal with attack
MASK	No	Partial Unlikability	Yes	Message relay attack, Timing analysis attack

VIII. CONCLUSION

In this paper, we proposed an unobservable routing protocol USOR [6] based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection complete unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. This protocol help in examining performance of USOR, which shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes. we propose trust based mechanism to overcome DoS, man in middle, black hole, sink hole, worm hole attacks.

REFERENCES

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

[19] 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.

[20] 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.

[21] Shao-Shan Chiang, , Chih-Hung Huang, and Kuang-Chiung Chang, "A Minimum Hop Routing Protocol for Home Security Systems Using Wireless Sensor Networks," *IEEE Transactions on Consumer Electronics*, Vol. 53, No. 4,

NOVEMBER 2007.

[22] Huei-Wen Ferng,Rachmarini, D.,"A secure routing protocol for wireless sensor networks with consideration of energy efficiency/Network Operations and Management Symposium (NOMS)," 2012 IEEE .

[23] Kui Ren, Ming Gu, and Zhiguo Wan (2012) "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE Trans. on Wireless Communications, vol. 11, no. 5, pp. 1922-1932.

[24] 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

[25] J. Kong and X. Hong, "ANODR: anonymous on demand routing with untraceable routes for mobile adhoc networks", in Proc. ACM MOBIHOC' 03.

[26] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks", Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.

[27] K. E. Defrawy and G. Tsudik, ―ALARM: anonymous location-aided routing in suspicious MANETs,‖ IEEE Trans Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011

[28] Routing Security in Wireless Ad Hoc Networks, Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati, 0163-6804/02 IEEE 2002