Wormhole Detection using RBS based Ad-hoc on-Demand Multipath Distance Vector as Routing Protocol in MANETs

Neha Chandrima, Sunil Phulre, Vineet Richharia

Abstract— Mobile Adhoc Networks (MANETs) is a collection of mobile nodes. Due to globalization and revolution in communication technology, growth in the deployment of wireless and mobile communication networks have been noticed. Several challenges and issues are raised by researchers working in the field of Dynamic topology and infrastructure less MANETs. Such facility generates easy installation of Ad hoc networks and provides node stability without loss of connection. In such facility packet dropping is a serious challenge for quality performance of MANETs. Exhaustive literature survey reveals that MANETs generally suffer from security attacks such as black hole attack, wormhole attack and malicious attack due to the packet dropping problems. For the minimization attack and packet dropping researchers have provided the solutions like authentication, reputation based scheme, certification based scheme, passive feedback scheme, ack-based scheme etc. In certification based scheme, a problem of huge overhead due to extra authentication of packet is noticed. Also, the problem of issuing certificate and authentication of certificate at each node are the great challenge to be resolved. To resolve these challenges, Entropy based reference-broadcast synchronization (RBS) scheme is used in which nodes send reference beacons to their neighbors using physical-layer broadcasts. The characteristic entropy changes are used to construct a threshold based detector for fast worms. Proposed scheme is implemented in NS2 simulator and its result shows the effect of normal behavior and improvement of performance after application of this scheme. In this, 50 nodes are used for simulation process and performance is evaluated by packet delivery ratio and normalized load using ad-hoc on-demand multipath distance vector (AOMDV) as routing protocol. This entropy based scheme, successfully minimizes the communication cost by reducing the number of overhead packets, removes the node ambiguity in broadcast synchronization process and minimizes packet dropping also.

Index Terms— AOMDV Protocol, Dynamic Topology, Mobile Ad-hoc Networks, Reference-broadcast Synchronization

I. INTRODUCTION

MANET is a self-configuring network of mobile nodes that constitutes a network capable of dynamically changing topology. The main objective of such type of network is to provide rapid means of communication. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of this network is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations as the traditional routers in fixed networks. In this, to maintain connectivity , all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority as it is not available. Therefore, a network-layer protocol designed for such self-organized networks must enforce connectivity and security requirements to assure the undisrupted operation of the higher layer protocol. Wireless communication technology have been developed with two main models namely: fix infrastructure based model, in which much of the nodes are mobile and connected through fixed backbone nodes using wireless medium, other model is Mobile Ad-hoc network. This model comprised of mobile nodes that are self-organizing and cooperative to ensure efficient and accurate packet routing between nodes. There are no specific routers, servers, access points for MANETs, Because of its fast and ease of deployment, robustness, and low cost, typical MANET applications can be find in several areas like military applications search and rescue operations, temporary networks within meeting rooms, airports, vehicle-to-vehicle communication in smart transportation, Personal Area Networks connecting mobile devices like mobile phones, laptops, smart watches, and other wearable computers etc. Design issue for developing a routing protocol for wireless environment with mobility is very different and more complex than those for wired network with static nodes [1]. Main problem in mobile adhoc network are limited bandwidth and frequent change in the topology. Although there are lots of routing protocols that can be used for unicast and multicast communication within the Mobile Ad hoc networks, it observes that any one protocol cannot fit in all the different scenarios, different topologies and traffic patterns of MANETs applications. Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems [2]. The flowchart shown in Fig.1

Manuscript Received March, 2014.

Neha Chandrima, PG student, Department of Computer Science and Engineering, Laxmi Narain College of Technology, Bhopal, India.

Sunil Phulre, Asst. Professor, Department of Computer Science and Engineering, Laxmi Narain College of Technology, Bhopal, India.

Dr. Vineet Richharia, HOD, Department of Computer Science and Engineering, Laxmi Narain College of Technology, Bhopal, India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

depicts the working of any general ad-hoc network.

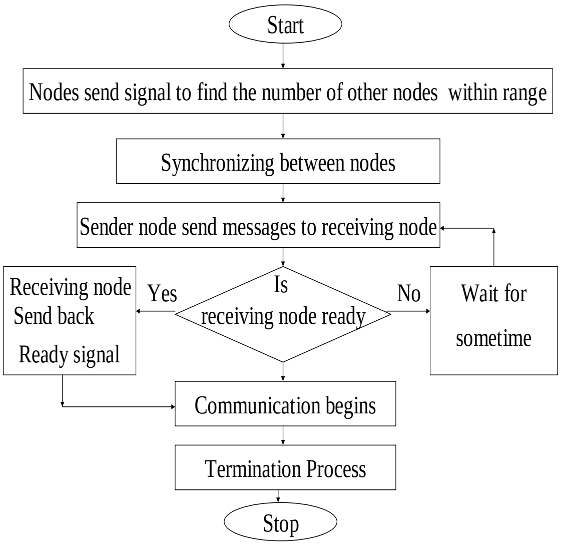
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Receiving node
Send back
Ready signal
Yes
Is
receiving node ready
No
Wait for
sometime
Communication begins
Termination Process
Stop

Fig.1: Flow chart of General Ad-Hoc Network

II. CLASSIFICATION OF ROUTING PROTOCOL

Routing protocols [3] typically fall under two classifications first one is unicast Routing Protocol, second one is multicast Routing Protocol. Different routing protocols try to solve the problem of routing in mobile ad hoc network in one way or the other. Unicast routing protocols are divided into proactive, reactive and hybrid routing protocols, and the multicast routing protocol are divided into proactive, reactive, and hybrid routing protocol. Figure 2 gives a classification of routing protocols.

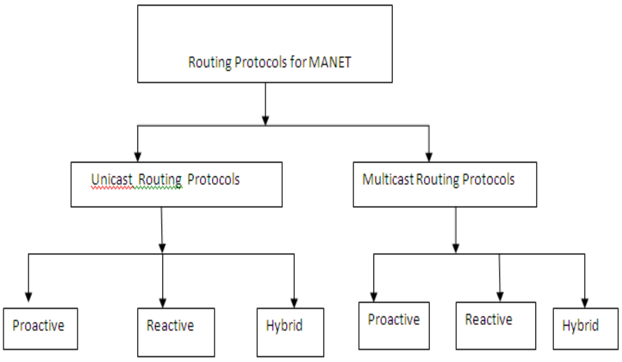
Routing Protocols for MANET
Unicast Routing Protocols
Multicast Routing Protocols
Proactive
Reactive
Hybrid
Proactive
Reactive
Hybrid

Fig.2 : Classification of Routing Protocols in MANET

III. SECURITY ISSUES IN MANET ROUTING

A great challenge to system security designers have been identified due to the following reasons:

- The wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering.
- The lack of an online trusted Third Party adds the difficulty to deploy security mechanisms.
- Mobile devices tend to have limited power consumption and computation capabilities which make it more vulnerable to denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms.
- In MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks [4].

The primary security services for MANETs are:
Authentication
Confidentiality,
Integrity
Non-repudiation
Availability

IV. AOMDV ROUTING PROTOCOL AND POSSIBLE ATTACKS

In Ad-hoc On-demand Multipath Distance Vector (AOMDV) each route discovery, multiple routes between source and destination are used. Use of alternate routes on a route failure is possible. New route discovery needed only when all routes fail. Fewer number of route discoveries exist. Reduction in delay and routing overhead are noted in this protocol. AOMDV performance relative to AODV is more than factor of two improvement in delay and also about 25% reduction in routing load. Marina et al. proposed multipath extensions to a well-studied single path routing protocol known as ad hoc on-demand distance vector (AODV). The resulting protocol is referred to as ad hoc on-demand multipath distance vector (AOMDV). The protocol guarantees loop freedom and disjointness of alternate paths. Performance comparison of AOMDV with AODV using ns-2 simulations shows that AOMDV is able to effectively cope with mobility-induced route failures. In particular, it reduces the packet loss by up to 40% and achieves a remarkable improvement in the end-to-end [6]. The attacks on networks come in many varieties and they can be grouped based on different characteristics. The following are some major attacks identified by researchers:

(a) Wormhole Attacks: In this attack ,a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. [Fig. 3]

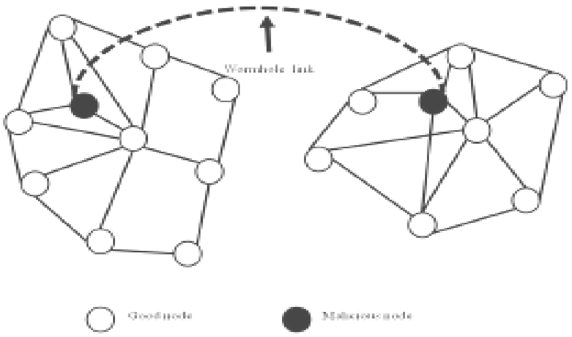

Fig. 3: Worm hole Attacks

(b) Sinkhole Attacks: Sinkhole attacks make use of the loopholes in routing algorithms of ad hoc networks and present themselves to adjacent nodes as the most attractive partner in a multiloop route.

(c) Black hole Attacks: In a Black hole attack [27], a malicious node uses a path outside the network to route messages to another compromised node at some other location in the net. Black holes are hard to detect because the path that is used to pass on information is usually not part of the actual network.

(d) Sleep Deprivation Torture Attack: Sleep deprivation attack [1] are most specific in wireless ad hoc networks, but may be encountered in conventional or wired network as well. The idea behind this attack is to request the services a certain node offers, over and over again, so it cannot go into an idle or power preserving state, thus depriving it of its sleep.

(e) Sybil attack: Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes, by doing so undermining the redundancy of many routing protocols. This type of attack is called Sybil attack

(f) Rushing attack : This type of attack is mostly directed against on-demand routing protocols based on the Dynamic Source Routing protocol. In Rushing attack, the attacker exploits the duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group and this will affect the average attack success rate.

V. REVIEW OF AVAILABLE LITERATURE

An extensive literature survey on the existing malicious attack in mobile adhoc network have been done and their findings are critically examined and concluded. The merits and limitations of their research findings are projected. Mary Anita et al. [7] reported that node misbehavior as Routing protocols for MANETs can be designed based on the assumption that all participating nodes are fully cooperative. Security issues are paramount in wireless networks even more so than in wired networks. A particularly devastating attack in wireless networks is the wormhole attack, where two or more malicious colluding nodes create a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. They analyzes the performance of reactive multicast routing protocol On Demand Multicast Routing Protocol (ODMRP) under the influence of worm hole nodes under different scenarios and design a Worm Hole Secure ODMRP by applying certificate based authentication mechanism in the route discovery process. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance. Jeremy Elson et al.[8] investigated that recent advances in miniaturization and low-cost, low power design have led to active research in large-scale network of small wireless, low-power sensors and actuators. Time synchronization is critical in sensor networks for diverse purposes including sensor data fusion, coordinated actuation, and power-efficient duty cycling. Though the clock accuracy and precision requirements are often stricter than in traditional distributed systems, strict energy constraints limit the resources available to meet these goals. They have also described a novel algorithm that uses this same broadcast property to federate clocks across broadcast domains with a slow decay in precision (3:68_2:57µsec after 4 hops).A significant improvement over the Network Time Protocol (NTP) under similar conditions was shown by this investigation. Adel Saeed Alshamrani et al. [9] concluded in their research work that the wormhole attack is hard to detect and can be easily implemented. An attacker may receive packets from one location in the network and tunnel them to the other end point in a different location and re-inject them into the network. Attackers can tunnel the packets by one of the following methods: encapsulating the packets, using out-of-bound links or using high power. If there are two or more malicious nodes in the network involved in a wormhole attack, the attack becomes more powerful. Satoshi Kurosawa et al.[10] **w**ormhole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged JREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper, Wormhole attack is analyzed and introduced the feature in order to define the normal state of the network. The authors have devised a new detection method based on dynamically updated training data. Yanchao Zhang et al.[11] concluded that non-cooperative behavior would cause the sharp degradation of network throughput. To address this problem, The authors have proposed a credit-based Secure Incentive Protocol (SIP) to stimulate cooperation among mobile nodes with individual interests. SIP can be implemented in a fully distributed way and does not require any pre-deployed infrastructure. SIP is also of low communication overhead by using a space-efficient Bloom filter. In addition, it is flexible and well adaptable to the network dynamics of MANETs. The effectiveness of SIP is validated through extensive simulations. Ning Song and Lijun Qian et al. [12] reported various routing attacks for single-path routing identified for wireless ad hoc networks and the corresponding counter measures have been proposed in the literature. However, the effects of routing attacks on multi-path routing have not been addressed. In this paper, the performance of multi-path routing under wormhole attack is studied in detail. The results show that multi-path routing is vulnerable to wormhole attacks. A simple scheme based on statistical analysis (SAM) is proposed to detect such attacks and to identify malicious nodes. Comparing to the previous approaches, no special requirements (such as time synchronization or GPS) are needed in the proposed scheme. Simulation results demonstrate that SAM successfully detects wormhole attacks and locates the malicious nodes in networks with different topologies and with different node transmission range. Moreover, SAM may act as a module in local detection agents in an intrusion detection system (IDS) for wireless ad hoc networks. Mahesh K. Marina and Sameer Das [6] developed an on-demand, multipath distance vector routing protocol for mobile ad hoc networks. Specifically,They proposed multipath extensions to a well-studied single path routing protocol known as ad hoc on-demand distance vector (AODV). The resulting protocol is referred to as ad hoc on-demand multipath distance vector (AOMDV). The protocol guarantees loop freedom and disjointness of alternate paths. Performance comparison of AOMDV with AODV using ns-2 simulations shows that AOMDV is able to effectively cope with mobility-induced route failures. In particular, it reduces the packet loss by up to 40% and achieves a remarkable improvement in the end-to-end delay (often more than a factor of two). AOMDV also reduces routing overhead by about 30% by reducing the frequency of route discovery operations. Jaiswal and Sharma [13] reported a comparison of relative clustered entropy based AOMDV as routing protocol in wormhole detection and they claimed that there is significant improvement of performance after the application of their proposed scheme.

VI. PROPOSED SCHEME

In this research work, Relative entropy calculation based reference-broadcast synchronization scheme is used in which nodes send reference beacons to their neighbors using physical-layer broadcasts. In first simulation, AOMDV protocol having two wormhole nodes on NS2.34 produces output in the form of trace files and graphs. In second simulation, the AOMDV with entropy and RBS scheme having two wormholes on NS2.34 produces output in the form of trace files and graphs.

VII. SIMULATION AND RESULT ANALYSIS

To investigate the effectiveness of the proposed scheme in defending against packet dropping in malicious attacks, the simulation on a simplified topology was carried out using Network Simulator NS-2.34

AOMDV Protocol Files

Header files:

- aomdv.h
- aodv_mpacket.h
- aodv_mqueue.h
- aodv_mtable.h
- aodv_mlogs.h

Source code files

- aomdv.cc
- aodv_mqueue.cc
- aodv_mtable.cc
- aodv_mcast.cc

AOMDV Implementation File

Header files:

- Idsaodv.h
- idsaodv_rqueue.h
- idsaodv_rtable.h

Source code files

- Idsaodv.cc
- idsaodv_logs.cc
- idsaodv_rqueue.cc
- idsaodv_rtable.cc
- idsaodv_semih.cc

Tcl file

- neha_prog2.tcl

Nam File

- resMD-New.nam

The main code is implemented in aomdv.cc and the functions are declared in aomdv.h. In aodv_mpacket.h, the AOMDV message formats (JoinRREQ, JOinRREP, and HELLO) are defined. Simulation scenario of entropy basedscheme on pause time 1 seconds and 10 seconds are shown in Fig. 4 and Fig. 5 respectively.

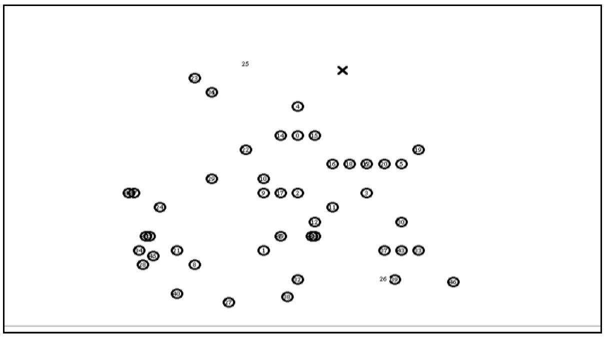

Fig. 4 Simulation scenario on pause time 1 second

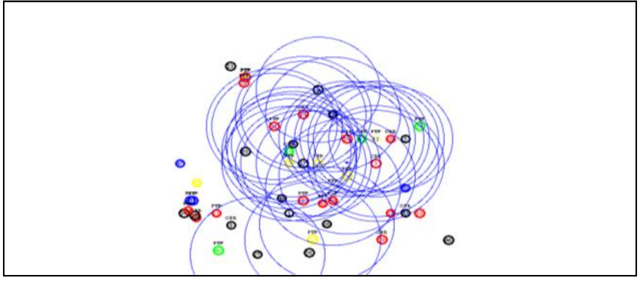

Fig. 5 Simulation scenario on pause time 10 second

A sample result obtained using proposed scheme plotted in the form of X graph is given in Fig. 6.

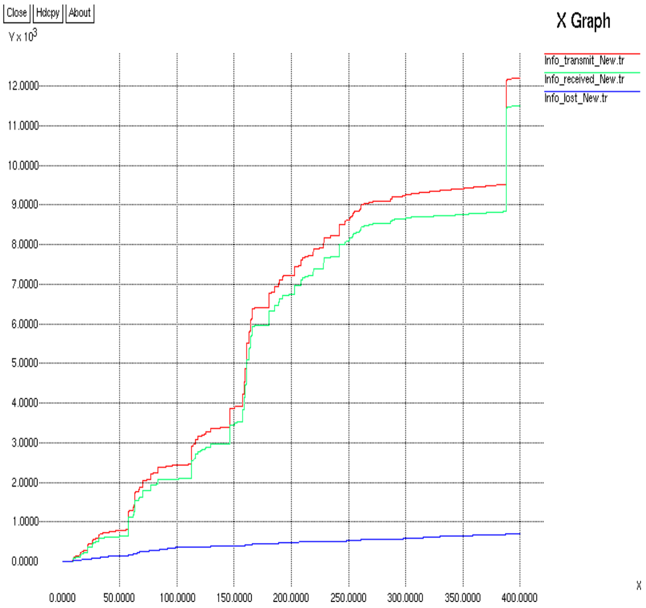

Fig.6: X graph results depicting transmit, received lost packet and drop packet in route advertisement

VIII. CONCLUSION

Evaluation of performance of AOMDV using clustered entropy based approach has been emerged as powerful technique in wormhole detection. In present work, Clustered entropy based, Reference Broadcast Synchronization technique is used as successful technique for node synchronization. From this study, It can be reported that entropy calculation scheme of detecting abnormal node reduces the relative computing overheads and communication cost. And RBS minimizes the communication cost by reducing the number of overhead packets for node authentication in mobile ad hoc networks. The limitation like more authentication of nodes is solved by Entropy calculation based scheme.

The study can be extended to incorporate in finding wormhole node by calculating entropy at each node. Researchers have yet to investigate it at each node and felt difficult to achieve due to high mobility and node identity.

ACKNOWLEDGMENT

Authors are thankful to Prof. Sanjay Sharma and Mr. G.P. Patel,OIST Bhopal for providing technical supports, discussions and positive criticisms during preparation of manuscript.

REFERENCES

1. Shuyao Yu, Youkun Zhang , Chuck Song and Kai Chen" A security architecture for Mobile Ad Hoc Networks" Proceedings of the II ACM Mobi HOC, 2001
2. T. Fahad, D. Djenouri and R. Askwith. "On detecting Packets Droppers in MANET: a Novel Low Cost Approach", Proceeding. III International Symposium on Information Assurance and Security, Manchester, UK August 2007.
3. Tony Larsson, Nicolas Headman; A report on "Routing Protocols in Wireless Ad Hoc Networks: A Simulation Study"1998.
4. M. Amitabh, "Security and quality of service in ad hoc wireless networks", Cambridge University Press I edition, March 2008.
5. T R Andel and A Yasinsac, "Surveying Security Analysis Techniques in MANET Routing Protocols", IEEE Communication Surveys & Tutorials, 9,4 pp 70-84, Fourth Quarter 2007
6. Mahesh K. Marina and Sameer . Das "Ad hoc on-demand multipath distance vector routing" wireless communications and mobile computing, 2006; 6:969–988
7. E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj, B.Prabhu, "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks", in proceeding of IEEE communication 2011
8. Jeremy Elson, NLewis Girod and Deborah Estrin," Fine-Grained Network Time Synchronization using Reference Broadcasts" in proceeding of IEEE communication 2011.
9. Adel Saeed Alshamrani" PTT: Packet Travel Time Algorithm in Mobile Ad Hoc Networks", in proceeding of IEEE 2011
10. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Wormhole Attack on MAODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." in proceeding of IEEE 2011.
11. Y. Zhang, W. Lou, W. Liu and Y. Fang, "A secure incentive protocol for mobile ad hoc networks", Wireless Networks journal, 13(5): pp569-582, October 2007.
12. Ning Song and Lijun Qian, Xiangfang L WINLAB "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach" Parallel and Distributed Processing Symposium, Proceedings, 19th IEEE International ,April 2005.
13. Jaiswal R and Sharma S, " Relative cluster entropy based wormhole detection using AOMDV in adhoc networks" Computational intelligence and communication networks (CICN) 2012 Proceeding of Fourth International conference, held at Mathura, Nov.2012, pp 747-752