Countermeasures of Network Layer Attacks in MANETs

Mangesh M Ghonge
Assistant Professor
Computer Science & Engg Department
JDIET, Yavatmal (MS), India

Pradeep M Jawandhiya
Associate Professor
Computer Science & Engg Department
JDIET, Yavatmal (MS), India

Dr. M S Ali
Principle
PRMIT, Badnera (MS), India

ABSTRACT
Security is an essential requirement in mobile ad hoc network (MANETs).In this paper, we proposed the survey of countermeasures of all security attacks of network layer in MANETs. To the best of our knowledge, this is the first paper that explaining all the existing countermeasures of network layer attacks in MANETs. The countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks.

Keywords
MANET, Security attacks, Network Layer

1. INTRODUCTION
Security is an essential service for wired and wireless network communications. The success of MANET strongly depends on whether its security can be trusted. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation.

2. DEFENCE AGAINST BLACKHOLE ATTACKS
A DPRAODV (Detection, Prevention and Reactive AODV) [2] is designed as a countermeasure to the blackhole attack. Two authentication mechanisms [4], based on the hash function is proposed to identify multiple black holes cooperating with each other. Wait and check the replies mechanism [3] is also proposed to find a safe route for packets. TOGBAD [5] a new centralized approach is proposed to identify nodes attempting to create a black hole. Security-aware ad hoc routing protocol (SAR) [5], is also proposed which can be used to defend against blackhole attacks.

Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node.

A DPRAODV (Detection, Prevention and Reactive AODV) is designed to prevent security threats of blackhole by notifying other nodes in the network of the incident. The simulation results in ns2 demonstrate that this protocol not only prevents blackhole attack but consequently improves the overall performance of (normal) AODV in presence of black hole attack.

Two authentication mechanisms, based on the hash function, the Message Authentication Code (MAC) and the Pseudo Random Function (PRF), are proposed to provide fast message verification and group identification, identify multiple black holes cooperating with each other and to discover the safe routing avoiding cooperative black hole attack.

To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. Computer simulation using GLOMOSIM shows that this protocol provides better performance than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

TOGBAD a new centralized approach, using topology graphs to identify nodes attempting to create a black hole. In this, use well-established techniques to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network. In this approach, we have to consider a node generating fake routing information as malicious. Therefore, we have to trigger an alarm if the plausibility check fails. Furthermore, there is a present promising first simulation result. With this new approach, it is possible to already detect the attempt to create a black hole before the actual impact occurs.

Security-aware ad hoc routing protocol (SAR) [54] can be used to defend against blackhole attacks. The security-aware ad hoc routing protocol is based on on-demand protocols, such as AODV or DSR. In SAR, a security metric is added into the RREQ packet, and a different route discovery procedure is used. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. At intermediate nodes, if the security metric or trust level is satisfied, the node will process the RREQ packet, and it will propagate to its neighbors using controlled flooding. Otherwise, the RREQ is dropped. If an end-to-end path with the required security attributes can be found, the destination will generate a RREP packet with the specific security metric. If the destination node fails to find a route with the required security metric or trust level, it sends a notification to the sender and allows the sender to adjust the security level in order to find a route.

3. DEFENSE AGAINST WORMHOLE ATTACKS
A cluster based counter-measure [6] is proposed as countermeasure for the wormhole attack. Wormhole Attack Prevention (WAP) without using specialized hardware [7] is

proposed to prevent the wormhole attack. A TrueLink mechanism is proposed which is a timing based countermeasure to the wormhole attack. A packet leash protocol [10] is designed as a countermeasure to the wormhole attack. The SECTOR mechanism [8] is proposed to detect wormholes without the need of clock synchronization. Directional antennas [9] are also proposed to prevent wormhole attacks.

A cluster based counter-measure is proposed as countermeasure for the wormhole attack that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET.

Wormhole Attack Prevention (WAP) without using specialized hardware is proposed to prevent the wormhole attack. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. Simulation results show that wormholes can be detected and isolated within the route discovery phase.

TrueLink is a timing based countermeasure to the wormhole attack. Using TrueLink, a node *i* can verify the existence of a direct link to an apparent neighbor, *j*. Verification of a link $i \leftrightarrow j$ operates in two phases. In the rendezvous phase, the nodes exchange nonces αj and βi. This is done with tight timing constraints, within which it is impossible for attackers to forward the exchange between distant nodes

Packet leashes are proposed to detect wormhole attacks. A leash is the information added into a packet to restrict its transmission distance. A temporal packet leash sets a bound on the lifetime of a packet, which adds a constraint to its travel distance. A sender includes the transmission time and location in the message. The receiver checks whether the packet has traveled the distance between the sender and itself within the time frame between its reception and transmission. Temporal packet leashes require tightly synchronized clocks and precise location knowledge. In geographical leashes, location information and loosely synchronized clocks together verify the neighbor relation.

The SECTOR mechanism is based primarily on distance-bounding techniques, one-way hash chains, and the Merkle hash tree. SECTOR can be used to prevent wormhole attacks in MANET without requiring any clock synchronization or location information. SECTOR can also be used to help secure routing protocols in MANET using last encounters, and to help detect cheating by means of topology tracking.

Directional antennas are also proposed as a countermeasure against wormhole attacks. This approach does not require either location information or clock synchronization, and is more efficient with energy.

4. DEFENSE AGAINST IMPERSONATION ATTACK

A multifactor authentication framework is proposed that extends the cryptographic link, binding an entity to a physical node device. ARAN [11] can be used to defend against impersonation and repudiation attacks.

A multifactor authentication framework is achieved by using two distinct authentication factors; certified keys and certified node characteristics. Although the proposed framework requires additional sensing capabilities from the MANET nodes, it provides the additional confidence level required for node authentication in critical applications.

ARAN provides authentication and non-repudiation services using predetermined cryptographic certificates for end-to-end authentication. In ARAN, each node requests a certificate from a trusted certificate server. Route discovery is accomplished by broadcasting a route discovery message *RDP* from the source node. The reply message *REP* is unicast from the destination to the source. The routing messages are authenticated at each intermediate hop in both directions.

5. DEFENSE AGAINST MODIFICATION ATTACKS

A new key management scheme [12] is implemented in NTP protocol. The security protocol SEAD [13] is used here as an example of a defense against modification attacks.

A new key management scheme is implemented in NTP protocol, since Node Transition Probability (NTP) based algorithm provides maximum utilization of bandwidth during heavy traffic with less overhead. NTP determines stable routes using received power, but the packet delivery cannot be guaranteed since it is a non secured protocol. The proposal detects the modification, impersonation attacks and TTL attacks and, avoids the effects of malicious node and determines appropriate measures to discard such malicious nodes in dynamic condition.

The security protocol SEAD is used here as an example of a defense against modification attacks. Similar to a packet leash [15], the SEAD protocol utilizes a one-way hash chain to prevent malicious nodes from increasing the sequence number or decreasing the hop count in routing advertisement packets. In SEAD, nodes need to authenticate neighbors by using TESLA broadcast authentication or a symmetric cryptographic mechanism. Specifically, in SEAD, a node generates a hash chain and organizes the chain into segments of m elements as ($h0$, $h1$, ..., hm_i1), ..., (hkm, hkm+1, ..., hkm+m_i1), ..., hn, where $k = n\ m - i$, m is the maximum network diameter, and i is the sequence number.

6. DEFENSE AGAINST DENIAL OF SERVICE ATTACKS

A DoSP-MAC protocol [14] is proposed to improve the fairness of the network. A novel scheme which is based on a firewall is proposed as countermeasure. A DoS mitigation technique [15] that uses digital signature is proposed to prevent DoS attack. Also proposed an efficient on-the-fly search technique [16] to trace back DoS attackers.

In wireless ad hoc networks, the performance of the media access control (MAC) protocol has significant impact on the overall network performance. In contention-based MAC protocols, nodes' access to the shared channel is not synchronized, and they contend for the channel whenever there are packets in their buffers ready to be sent. To reduce self contention, Fast-Forward Mechanism and Quick Exchange Mechanism are being used but these mechanisms aggravate the fairness problem. Thus it will lead to Denial of Service attacks because the last winner is always favored among local contending nodes, a continuously transmitting node can always

capture the channel and cause other nodes to back off endlessly. Here, a DoSP-MAC protocol is proposed to improve the fairness of the network thereby enhance its performance. This can drastically improve the medium utilization.

A novel scheme which is based on a firewall. This firewall can distinguish the attack packets from the packets sent by legitimate users based on the marking value on the packet, and thus filter out most of the attack packets. Compared to other packet-marking based solutions, our scheme is very effective and has a very low deployment cost. In the implementation of this scheme we would require the cooperation of only about 10% of the Internet routers in the marking process, and server to generate encrypted marking for secured transmission. The scheme allows the firewall to Detected and prevents the DDoS attacks from the first packet itself.

The mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification. Since nodes are selfish, they may not perform the verification so that they can avoid paying the overhead. A bad packet that escapes verification along the whole network path will bring a penalty to all its forwarders. A network game can be formulated in which nodes along a network path, in optimizing their own benefits, are encouraged to act collectively to alter out bad packets. Analytical results show that Nash equilibrium can be attained for players in the proposed game, in which significant benefits can be provided to forwarders such that many of the bad packets will be eliminated by verification.

In this mechanism, to use an efficient on-the-fly search technique to trace back DoS attackers. Our scheme is based on small world concept and effectively extends *Contacts* [3] for MANET utilizing location information. In addition, to deal with address spoofing problems in DoS attacks, we use Traffic Patterns Matching (TPM) [5] and propose to use Traffic Volume Matching (TVM) as matching-indepth to identify an attacker. We also processing innetwork processing and directional expanded ring search to reduce communication overhead in attacker traceback. We show that our scheme successfully trace back attacker using both TPM and TVM.

7. DEFENSE AGAINST GRAYHOLE ATTACKS

An aggregate signature algorithm [17] is proposed to trace packet dropping nodes.

In the proposed mechanism, firstly, DSR protocol, aggregate signature algorithm and network model were introduced. Secondly, we proposed to use aggregate signature algorithm to trace packet dropping nodes. The proposal was consisted of three related algorithms: the creating proof algorithm, the checkup algorithm and the diagnosis algorithm. The first was for creating proof, and the second was for checking up source route nodes, and the last was for locating the malicious nodes. Finally, the efficiency of the proposal was analyzed. The simulation results using ns-2 show that in a moderately changing network, most of the malicious nodes could be detected, the routing packet overhead was low, and the packet delivery rate has been improved.

8. DEFENSE AGAINST SYBIL ATTACKS

A robust Sybil attack detection framework [18] is proposed for MANETs based on cooperative monitoring of network activities.

In this mechanism, we do not require designated and honest monitors to perform the Sybil attack detection. Each mobile node in the network observes packets passing through it and periodically exchanges its observations in order to determine the presence of an attack. Malicious nodes fabricating false observations will be detected and rendered ineffective. Our framework requires no centralized authority and, thus, is scalable in expanding network size. Privacy of each mobile node is also a consideration of our framework. Our preliminary experimental results yield above 80% accuracy (true positives) and about 10% error rate (false positives).

9. DEFENSE AGAINST PACKET DROP ATTACKS

A two folded approach [19], to detect and then to isolate such nodes is proposed. A new approach [20] for detecting misbehaving nodes that drop data packets in MANET. Also propose a solution to protect control packets of reactive source routing protocols against. Propose an obligation-based model called fellowship to mitigate the flooding and packet drop attacks

A two folded approach, to detect and then to isolate such nodes is proposed which becomes the part of the network to cause packet dropping attacks. First approach will detect the misbehavior of nodes and will identify the malicious activity in network, and then upon identification of nodes misbehavior in network other approach will isolate the malicious node from network.

This proposed scheme consists of two stages the monitoring stage in which each node monitors its direct neighbours with respect to forwarding data packets of a traffic session in the network, and the decision stage, in which direct neighboring nodes decide whether the monitored node misbehave or not. Our new approach is able to detect the misbehavior in case of power control employment, with a low communication overhead compared to the existing approaches.

In this countermeasure, a solution to protect control packets of reactive source routing protocols against. Most current proposals focus on data packets. Nonetheless, dropping control packets may be beneficial for selfish nodes and malicious ones as well. For example, simply by dropping RREQ (Route Request) packets a selfish node could exclude itself from routes and thereby avoid receiving data packets to forward. Similarly, a malicious could drop RERR (Route Error) packets to keep the use of failed routes, potentially resulting in a denial of service. Our solution could be intergraded with any source routing protocol. For the implementation in this work, we have chosen one of the most secure protocols, namely ENDAIRA. We assess our solution by an extensive simulation study.

In this proposed mechanism, an obligation-based model called *fellowship* to mitigate the flooding and packet drop attacks. We also explain how the fellowship model identifies and penalizes both the malicious and selfish nodes respectively in mobile ad hoc networks (MANET). The main advantages of our model are: it unifies the framework to defend both flooding and packet drop attacks, it identifies and expels the malicious and selfish nodes that fail to contribute their resources, and rejoins the repenting malicious and selfish nodes into the

network. In addition, our technique does not rely on any centralized authority or tamper-proof hardware.

10. DEFENSE AGAINST BYZANTINE ATTACKS

A secure on-demand MANET routing protocol, named Robust Source Routing (RSR) [21] is proposed as countermeasure of Byzantine attacks. A Chord mechanism is proposed which is a distributed hash table (DHT).

A secure on-demand MANET routing protocol, named Robust Source Routing (RSR). In addition to providing data origin authentication services and integrity checks, RSR is able to mitigate against intelligent malicious agents which selectively drop or modify packets they agreed to forward. Simulation studies confirm that RSR is capable of maintaining high delivery ratio even when a majority of the MANET nodes are malicious.

Chord is a distributed hash table (DHT) that requires only O(log n) links per node and performs searches with latency and message cost O(log n), where n is the number of peers in the network. Chord assumes all nodes behave according to protocol. We give a variant of Chord which is robust with high probability for any time period.

11. DEFENSE AGAINST LOCATION DISCLOSURE ATTACKS

A new approach [22] which uses geometric constraints and heuristics to find node positions efficiently. Terminode routing [23] is presented to addresses issues of location disclosure attack.

Location privacy is an important issue in ad hoc networks. So to analyze what extent an attacker can track the precise location of a node, assuming a powerful attacker model where an attacker knows all neighbor relationships plus information on node distances. We present a new approach which uses this information and uses geometric constraints and heuristics to find node positions efficiently. The quality of our results is discussed and compared to other approaches. Based on the localization precision that such an "omniscient" attacker can reach, we will be able to evaluate the quality of future, more realistic attack models.

Terminode routing, presented here, addresses these issues. It uses a combination of location-based routing (Terminode Remote Routing, TRR), used when the destination is far, and link state routing (Terminode Local Routing, TLR), used when the destination is close. TRR uses anchored paths, a list of geographic points (not nodes) used as loose source routing information. Anchored paths are discovered and managed by sources, using one of two low overhead protocols: Friend Assisted Path Discovery and Geographical Map-based Path Discovery. Our simulation results show that terminode routing performs well in networks of various sizes. In smaller networks, the performance is comparable to MANET routing protocols. In larger networks that are not uniformly populated with nodes, terminode routing outperforms existing location-based or MANET routing protocols.

12. CONCLUSION AND FUTURE WORK

In this paper we present the countermeasures of different attacks of network layer. Vulnerability of nodes, absence of infrastructure and dynamic changing topology make the security of mobile ad hoc network more difficult. With development of computing environment, the security attacks detection/prevention techniques are also increasing. In this paper, we tried to inspect existing countermeasures of network layer security attacks in Mobile Ad hoc network. For future work, we are finding some points that can be further explored to protect the MANET from network layer security attacks.

13. REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[2] Payal N. Raj and Prashant B. Swades, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET" , IJCSI International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814.

[3] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007).

[4] Zhao Min and Zhou Jiliu1, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", 2009 International Symposium on Information Engineering and Electronic Commerce.

[5] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs Networks ," 32nd IEEE Conference on Local Computer Networks 0742-1303/07 $25.00 © 2007 IEEE.

[6] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki,"A New Cluster based wormhole intrusion detection algorithm for MANET", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009

[7] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung," WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing

[8] S. Capkun, L. Buttyan, and J. Hubaux, Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. *Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[9] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", *Proc. of Networks and Distributed System Security Symposium* (NDSS), 2004.

[10] Y. Hu, A Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks." *Proc. of IEEE INFORCOM*, 2002.

[11] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. *Proc. of IEEE International Conference on Network Protocols* (ICNP), pp. 78-87, 2002

[12] Vaithiyanathan, Gracelin Sheeba.R, Edna Elizabeth. N, Dr.S.Radha, "A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm ", 2010 International Conference on Recent Trends in Information, Telecommunication and Computing 978-0-7695-3975-1/10 $25.00 © 2010 IEEE.

[13] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks. *Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA'02), pp. 3-13, 2002.

[14] R. Gunasekaran and V. Rhymend Uthariaraj, "Prevention of Denial of Service Attacks and Performance Enhancement in Mobile Ad hoc Networks ", 2009 Sixth International Conference on Information Technology: New Generations 978-0-7695-3596-8/09 $25.00 © 2009 IEEE

[15] Xiaoxin Wu and David K. Y. Yau, "Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach",. *ASIACCS'07,* March 20-22, 2007, Singapore.

[16] Yongjin Kim, Vishal Sankhla, Ahmed Helmy1," Efficient Traceback of DoS Attacks using Small Worlds in MANET", Proc. 2004 IEEE.

[17] Gao Xiaopeng and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", 2007 IFIP International Conference on Network and Parallel Computing – Workshops @ 2007 IEEE.

[18] Athichart Tangpong, George Kesidis, Hung-yuan and Hsu Ali Hurson, "Robust Sybil Detection for MANETs " 978-1-4244-4581-3/09/$25.00 ©2009 IEEE.

[19] Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema, Attique Ahmed," Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks", 2008 International Seminar on Future Information Technology and Management Engineering 978-0-7695-3480-0/08 $25.00 © 2008 IEEE.

[20] Tarag Fahad1, Djamel Djenouri2, Robert Askwith1, "On Detecting Packets Droppers in MANET: A Novel Low Cost Approach "Third International Symposium on Information Assurance and Security 0-7695-2876-7/07 $25.00 © 2007 IEEE

[21] Claude Cr´epeau, Carlton R. Davis and Muthucumaru Maheswaran, "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes ", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 0-7695-2847-3/07 $20.00 © 2007 IEEE.

[22] Sergey Chapkin, Boto Bako, Frank Kargl, Elmar Schoch," Location Tracking Attack in Ad hoc Networks based on Topology Information ", 1-4244-0507-6/06/$20.00 ©2006 IEEE.

[23] Ljubica Blazevic, Jean-Yves Le Boudec and Silvia Giordano, "A Location-Based Routing Method for Mobile Ad Hoc Networks ", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 4, NO. 2, MARCH/APRIL 2005.

14. AUTHOR BIOGRAPHIES

Mangesh M Ghonge was born in India in 1984; He received his BE degree in Computer Science & Engineering from the Computer Science & Engineering Department in 2007. He is pursuing M Tech degree in Computer Science & Engineering. His research interest includes security in wireless networks, Ad-Hoc networks, and network protocols. Also includes implementation of open source software. He acquired knowledge in sciences/skills that covers areas of Computer Science, Networking, Databases and Programming, and more. He is life member of IACSIT, IAENG and CSTA.

Pradip M. Jawandhiya is Associate Professor & Head of Department of Computer Science & Engineering at Jawaharlal Darda Institute of Engineering & Technology,Yavatmal. He did his B.E.(Computer Engineering) in 1993 & M.E. (Computer Science & Engineering) in 2001 from Prof. Ram Meghe Institute of Technology & Research, Badnera – Amravati. He is currently Ph.D. Scholar in Computer Science & Engineering from SGB Amravati University, Amravati. He is life member of I.S.T.E.; C.S.I. and Fellow of I.E.T.E., Member IEEE, Member IACSIT.

Dr. M.S. Ali is Principal at Prof. Ram Meghe College of Engineering & Management, Badnera – Amravati. He did his B.E (Electrical) in 1981 from Govt. College of Engineering, Amaravati, M.Tech. from I.I.T. Bombay in 1984 and Ph.D. in the faculty of Engineering & Technology of S.G.B. Amravati University in 2006 in the area of e-Learning. He is life member of ISTE, New Delhi., Fellow of I.E.T.E, New Delhi Chairman of IETE Amravati Center and Fellow of I.E.(India).