IJCSC 0973-7391 Vol 6 • Number 2 April - Sep 2015 pp. 364-367 **Impact Factor: 2.5** **Available at** www.csjournals.com

IDS and its Routing Protocols in MANET

Suraj Pal
Assistant professor, Deptt. of computer science, University College, KUK, India
suraj.nehra1@gmail.com

Abstract: Although Intrusion Detection technology (IDS) is undeveloped and should not be measured as a complete security, we believe it can play a major role in overall security architecture. Many efforts were made to secure wireless ad hoc networks (WAHNs), but due to their unique ad hoc nature and strict constraints, finding an optimal and complete security solution is still a research challenge. In this paper we will review the Intrusion Detection technology (IDS), IDPS and its principal types, MANET and its different routing protocols. We will study the two protocols AODV and DSR, and compared their performances on various performance parameters.
Keywords: IDS, IDPS, MANET, DSR, AODV.

I. INTRODUCTION

Intrusion detection is a security technique that tries to find out individuals who are trying to mistreat and break into a system without authorization and those who have genuine access to the system, but are abusing their rights. An intrusion detection system (IDS) is a computer system that vigorously monitors the system and user actions in the network system and computer systems in order to detect intrusions. A wireless Mobile Ad hoc NETwork (MANET) does not need costly base stations or wired infrastructure. No of nodes within the radio range of each other can communicate directly or openly over the wireless links, while those that are distant use other nodes as relays. In MANETs, each host act as a router since route is mostly multi hop. Nodes in such a network move randomly, thus the network topology changes unpredictably and frequently. Many routing protocols have been planned for MANETs. In general, these protocols could be divided into three types: reactive, proactive, and hybrid. Reactive routing protocols [1, 2, 7, 8] are based on demand for data transmission. Proactive routing protocols or table-driven protocols react according to topology change, even if there is no traffic. They can significantly decrease the routing overhead when the traffic is trivial and the topology changes less dramatically, since they do not need to occasionally update route information and do not need to find and preserve the routes when there is no traffic. Hybrid methods combine reactive and proactive methods to find able or efficient routes.

II. ROUTING PROTOCOL in MANET

Fig. 1 is a classification of existing routing protocols in MANETs.

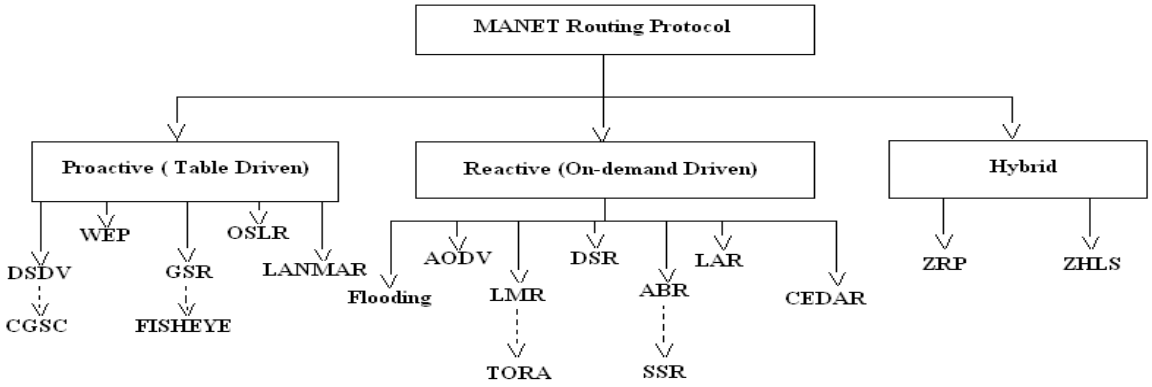


Fig. 1 Classification of MANET Routing Protocol

But our main center of attention will be on Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector routing protocol (AODV).

A. Dynamic Source Routing (DSR)

The key distinctive feature of DSR [8, 9] is the use of source routing. In source routing, the sender knows the entire hop-by-hop route to the destination. These all routes are stored in a route cache. The data packets hold the source route in the packet header. When a node in the ad hoc network try to send a data packet to a destination for which it does not already identify the route, it uses a route discovery process to dynamically find out such a route. Route discovery works by flooding the network with route request (RREQ) packets. Each node which receives an RREQ rebroadcasts it, unless it is the destination node or it has a route to the destination node in its route cache. Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to the novel

source node. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed throughout the network. The RREP route itself back to the source node by navigated this path backward. The route carried back by the RREP packet is cached at the source node for future use. If any link on a source route is broken, the source node is reported using a route error (RERR) packet. The source eliminates any route using this connection from its cache. A original route discovery process must be started by the source if this route is still needed. DSR makes very violent use of source routing and route caching. No particular mechanism to detect routing loops is needed. Also, some forwarding node caches the source route in a packet it forwards for possible future use.

B. Ad-hoc On-demand Distance Vector Routing (AODV)

AODV shares DSR's on-demand features in that it also determines routes on as desirable basis via a similar route discovery process. However, AODV allows a very different mechanism to manage routing information. It uses a conventional routing table, one entry per destination. AODV contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV depends on routing table entries to transmit an RREP back to the source and, then, to route data packets to the destination. AODV uses sequence numbers preserved at each destination to determine originality of routing information and to avoid routing loops. These sequence numbers are accepted by all routing packets. A key feature of AODV is the maintenance of time-based states in each and every node, concerning utilization of individual routing table entries. A routing table entry is terminated if not used recently. A set of all predecessor nodes is maintained for each and every routing table entry, signifying the set of all neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop connection or link breaks. Each and every predecessor node, forwards the RERR to its own set of all predecessors, hence successfully erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are proposed to notify all sources using a link when a failure in network occurs. Route error transmission in AODV can be imagined theoretically as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves. The current specification of AODV includes an optimization technique to manage the RREQ flood in the route discovery process. It uses a growing ring search initially to discover routes to an unidentified destination. In the growing ring search, increasingly larger neighborhoods are searched to find the destination node. The search is controlled by the Time-To-Live (TTL) field in the IP header of the RREQ packets. If the route to an earlier known destination is needed, the prior hop-wise distance is used to optimize the search process. This allows computing the TTL value used in the RREQ packets dynamically, by taking into thought the temporal locality of routes.

III. Comparison of DSR and AODV

There are some important differences in the dynamics of these protocols, which may give increase to significant performance differentials.

First, by virtue of source routing, DSR has access to extensively greater amount of routing information than AODV. Each intermediate or middle node can also discover routes to every other node on the route. immoral listening of data packet transmissions can also provide DSR access to an important amount of routing information. In particular, it can find out routes to every node on the source route of the data packet. In the absence of source routing and immoral listening, AODV can collect only a very limited amount of routing information. In particular, route learning is restricted only to the source of any routing packets being forwarded. This usually causes AODV to depend on a route discovery flood more frequently, which may carry considerable network overhead.

Second, to make use of route caching vigorously, DSR replies to each and every requests reaching a destination from a particular request cycle. Thus, the source learns various alternate routes to the destination, which will be useful in the case that the shortest route fails. Having access to several alternate routes saves route discovery floods, which is repeatedly a performance blockage. However, there may be a route reply flood. In AODV, on the other hand, the destination replies only once to the request incoming first and ignores the rest. The routing table maintains mainly one entry per destination.

Third, the current requirement of DSR does not contain any clear mechanism to hold hard routes in the cache, or prefer "fresher" routes when faced with various choices. Hard routes, if used, may start contaminate other caches. Some hard entries are indeed deleted by route error packets. But because of immoral listening and node mobility, it is possible that more caches are contaminated by hard entries than are removed by error packets. In contrast, AODV has a much more conventional approach than DSR. When faced with two choices for routes, the fresher route (based on destination sequence numbers) is always selected. Also, if a routing table entry is not used recently, the entry is expired.

Fourth, the route deletion activity using RERR is also conventional in AODV. By way of a predecessor list, the error packets reach each and every nodes using a failed link on its route to any destination.

A. Performance Metrics

Four major performance metrics are evaluated:

• Packet delivery fraction: - the ratio of the data packets transported to the destination nodes to those generated by the CBR source nodes; also, a related metric, received throughput (in kbps) at the destination has been evaluated in some cases.

• Average end-to-end delay of the data packets: - this includes all possible delays caused by buffering throughout route discovery latency, queuing at the interface queue, propagation, transfer times and retransmission delays at the MAC.

• Normalized routing load: - the number of routing packets broadcasted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

• Normalized MAC load: - Address Resolution Protocol (ARP), the number of routing packets, and control (e.g., RTS, CTS, ACK) packets transmitted by the MAC layer for each and every delivered data packet. Basically, it considers both routing overhead and the MAC control overhead.

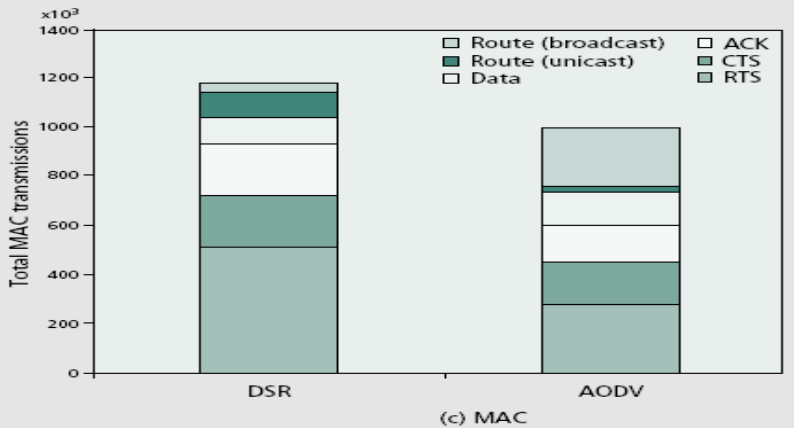
B. Comparison Results

Performance Metrics	DSR	AODV
Packet Delivery Fraction (%)	56.88	83.66
Average Delay (s)	1.36	0.26

a) Applications

Routing Packets	DSR	AODV
Route Requests	37,774	2,28,094
Route Reply	82,710	17,753
Route errors	26,591	9,808
Total	1,47,075	2,55,655

b) Routing



(c) MAC

IV. CONCLUSION

In this paper, we discussed the IDS, its principal types, MANET and its several routing protocols. We discussed the two protocols DSR and AODV and compared their performances on some performance parameters, two well-known on-demand routing protocols for ad hoc networks. DSR and AODV both use on-demand route discovery, but with various routing mechanics. In particular, DSR uses route caches and source routing and does not depend on periodic or timer-based activities. DSR develops caching aggressively and maintains several routes per destination. AODV, on the other hand, uses routing tables, destination sequence numbers, one route per destination and a mechanism to prevent loops and to determine freshness of routes.

REFERENCES

[1]. C. E. Perkins and E. M. Royer, "Ad Hoc On-demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., Feb. 1999, pp. 90–100.

[2]. C. Perkins, E. M. Royer, S. R. Das, and M. K. Marina. "Performance comparison of two on-demand routing protocols for ad hoc networks". IEEE Personal Communications Magazine special issue on Ad hoc Networking, pages 16 28, Feb. 2001.

[3]. Bo Sun, "Intrusion Detection in Mobile Ad hoc Networks",A & M University, May 2004.

[4]. Xia Wang, "Intrusion Detection Techniques in Wireless Ad Hoc Networks", IEEE Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC), 2006.

[5]. Abdulrahman Hijazi, Nidal Nasser "Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks" IEEE 2005.
[6]. Brutch, P.; Ko, C., "Challenges in intrusion detection for wireless ad-hoc networks," Proceedings of the IEEE Symposium on Applications and the Internet Workshops 27-31 Jan. 2003 pp. 368 – 373.
[7]. J.Broch, D. Johnson, and D. Maltz. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," IETF Internet draft, Oct. 1999.
[8]. D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," T. Imielinski and H. Korth, Eds. Mobile Computing, Kluwer, 1996.
[9]. K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication, Feb. 2007.