International Journal of Information Technology and Knowledge Management
January-June 2008, Volume 1, No. 1, pp. 45-50

IDS IN MANET AND ITS ROUTING PROTOCOL

Anil kumar, Arun Jain & Rakesh Sharma

Abstract

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

Keywords: IDS, IDPS, MANET, DSR, AODV.

I. Introduction

Intrusion detection [3] is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system, but are abusing their privileges. An intrusion detection system (IDS) is a computer system that dynamically monitors the system and user actions in the network and computer systems in order to detect intrusions A wireless Mobile Ad hoc NETwork (MANET) does not need expensive base stations or wired infrastructure. Nodes within the radio range of each other can communicate directly over the wireless links, while those that are far apart use other nodes as relays. In MANETs, each host must act as a router since routes are mostly *multihop*. Nodes in such a network move arbitrarily, thus the network topology changes frequently and unpredictably. Many routing protocols have been proposed for MANETs. In general, these protocols could be divided into three categories: *proactive*, *reactive*, and *hybrid*. *Proactive* routing protocols or *table-driven* protocols reacts according to topology change, even if there is no traffic. *Reactive* routing protocols [1, 2, 7, 8] are based on demand for data transmission. They can significantly reduce the routing overhead when the traffic is lightweight and the topology changes less dramatically, since they do not need to periodically update route information and do not need to find and maintain the routes when there is no traffic. *Hybrid* methods combine *proactive* and *reactive* methods to find efficient routes.

2. Routing Protocols in MANET

Figure 1 is a categorization of existing routing protocols in MANETs.

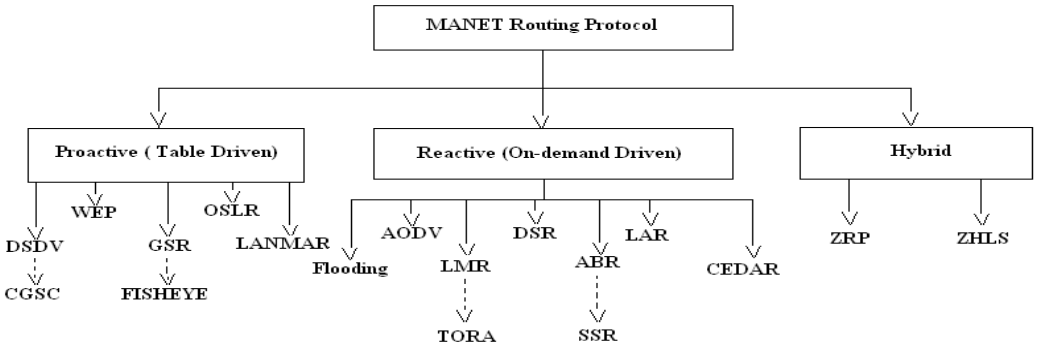


Figure 1: Classification of MANET Routing Protocol

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

A. Dynamic Source Routing (DSR)

The key distinguishing feature of DSR [8, 9] is the use of *source routing*. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a *route cache*. The data packets carry the source route in the packet header. When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a *route discovery* process to dynamically determine such a route. Route discovery works by flooding the network with *route request* (RREQ) packets. Each node receiving an RREQ rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the RREQ with a *route reply* (RREP) packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path backward. The route carried back by the RREP packet is cached at the source for future use. If any link on a source route is broken, the source node is notified using a *route error* (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed. DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any 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 characteristics in that it also discovers routes on an *as needed* basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple

route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. These sequence numbers are carried by all routing packets. An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is *expired* if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves. The recent specification of AODV includes an optimization technique to control the RREQ flood in the route discovery process. It uses an *expanding ring search* initially to discover routes to an unknown destination. In the expanding ring search, increasingly larger neighborhoods are searched to find the destination. The search is controlled by the Time-To-Live (TTL) field in the IP header of the RREQ packets. If the route to a previously known destination is needed, the prior hop-wise distance is used to optimize the search. This enables computing the TTL value used in the RREQ packets dynamically, by taking into consideration the temporal locality of routes.

3. COMPARISON OF DSR AND AODV

There are several important differences in the dynamics of these two protocols, which may give rise to significant performance differentials.

First, by virtue of source routing, DSR has access to a significantly greater amount of routing information than AODV. Each intermediate node can also learn routes to every other node on the route. Promiscuous listening of data packet transmissions can also give DSR access to a significant amount of routing information. In particular, it can learn routes to every node on the source route of that data packet. In the absence of source routing and promiscuous listening, AODV can gather only a very limited amount of routing information. In particular, route learning is limited only to the source of any routing packets being forwarded. This usually causes AODV to rely on a route discovery flood more often, which may carry significant network overhead.

Second, to make use of route caching aggressively, DSR replies to *all* requests reaching a destination from a single request cycle. Thus, the source learns many alternate routes to the destination, which will be useful in the case that the primary (shortest)

route fails. Having access to many alternate routes saves route discovery floods, which is often a performance bottleneck. However, there may be a possibility of a route reply flood. In AODV, on the other hand, the destination replies only once to the request arriving first and ignores the rest. The routing table maintains at most one entry per destination.

Third, the current specification of DSR does not contain any explicit mechanism to expire stale routes in the cache, or prefer "fresher" routes when faced with multiple choices. Stale routes, if used, may start polluting other caches. Some stale entries are indeed deleted by route error packets. But because of promiscuous listening and node mobility, it is possible that more caches are polluted by stale entries than are removed by error packets. In contrast, AODV has a much more conservative approach than DSR. When faced with two choices for routes, the fresher route (based on destination sequence numbers) is always chosen. Also, if a routing table entry is not used recently, the entry is expired.

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

A. Performance Metrics

Four important performance metrics are evaluated:

- *Packet delivery fraction* the ratio of the data packets delivered to the destinations to those generated by the CBR sources; also, a related metric, received throughput (in kilobits per second) at the destination has been evaluated in some cases.
- *Average end-to-end delay of data packets* This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.
- *Normalized routing load* the number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.
- *Normalized MAC load* the number of routing, Address Resolution Protocol (ARP), and control (e.g., RTS, CTS, ACK) packets transmitted by the MAC layer for each delivered data packet. Essentially, it considers both routing overhead and the MAC control overhead.

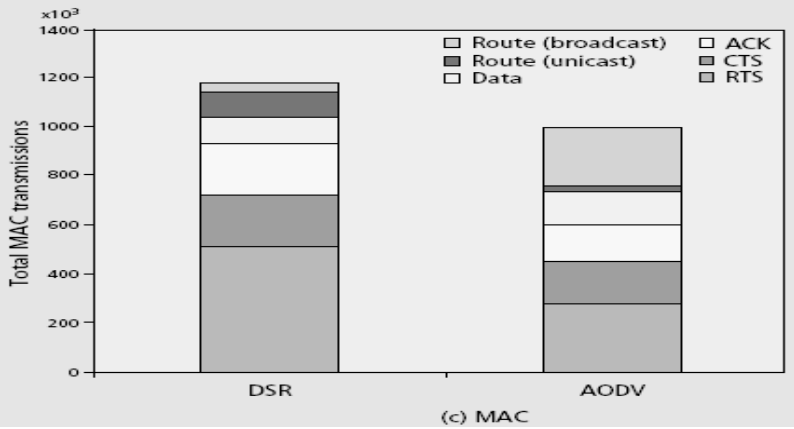
B. Comparison Results

a) Applications

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

b) Routing

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



CONCLUSION

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

REFERENCES

[1] C. E. Perkins and E. M. Royer, (February-1999), "Ad-hoc On-demand Distance Vector Routing," Proc. 2nd *IEEE Wksp. Mobile Comp. Sys. and Apps*., 90-100.

[2] C. Perkins, E. M. Royer, S. R. Das and M. K. Marina. (February-2001), "Performance Comparison of Two On-demand Routing Protocols for Ad-hoc Networks", *IEEE Personal Communications Magazine Special Issue on Ad-hoc Networking*, 16-28.

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

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

[5] Abdulrahman Hijazi and Nidal Nasser (2005), "Using Mobile Agents for Intrusion Detection in Wireless Ad-hoc Networks" IEEE.

[6] Brutch, P. and Ko C., (January-2003), "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," Proceedings of the IEEE Symposium on Applications and the Internet Workshops, 368-373.

[7] J. Broch, D. Johnson and D. Maltz. (October-1999), "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks," IETF Internet draft.

[8] D. Johnson and D. Maltz, (1996), "Dynamic Source Routing in Ad-hoc Wireless Networks," T. Imielinski and H. Korth, Eds. *Mobile Computing*, Kluwer.

[9] K. Scarfone and P. Mell, (February-2007), "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication.

Anil kumar
Department of Information Technology
HCTM, Kaithal, Haryana, INDIA
E-mail: akj_jakhar@yahoo.com

Arun Jain
Department of Computer Sc. & Engg.
HCTM, Kaithal, Haryana, INDIA
E-mail: erarunjain@rediffmail.com

Rakesh Sharma
Deptt. of Computer Sc. & Engg.
GJU, Hisar, Haryana, INDIA
E-mail: rakeshsharma3112@gmail.com