Journal of Computer Science 9 (10): 1420-1426, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1420.1426 Published Online 9 (10) 2013 (http://www.thescipub.com/jcs.toc)

LIGHTWEIGHT VIGILANT PROCEDURE TO IMPLEMENT SECURITY MEASURES IN HIGHLY ROVING MILITARY OPERATIONS

Udhayan, J. and Rajesh Babu

PPG Institute of Technology,
Faculty of Computer Science and Engineering, Anna University, Coimbatore Zone, India

Received 2013-04-23, Revised 2013-07-08; Accepted 2013-09-18

ABSTRACT

The performance of Mobile Ad hoc Network (MANET) becomes questionable in highly roving and mission critical application like military operation. Security measures like encryption, authentication, digital signature has been proposed for MANET. However all those mechanisms need some kind of static infrastructure and it is extremely difficult to implement such an infrastructure throughout the military mission. Therefore in this work, various zones in military operation is identified and Zone A is responsible for implementing robust security measures, Zone B and Zone C are identified to be at highly hostile and time critical environment. Therefore usage of highly complex security procedures at zone B & C may delay the operation to the extent of failure of the mission. Hence in this study, a lightweight vigilant procedure that suits the circumstances of Zone B & C is proposed, it has the capability of detecting the malicious entrant in the routing path. Moreover, it works either independently or dependently with the routing protocols like AODV based on the need. The proposed method has been compared with various successful security measures in Ad-hoc network and the results shows that the proposed method is very useful in adapting to the conditions of zone B & C.

Keywords: AD-HOC, MANET, AODV, S-AODV, ARAN

1. INTRODUCTION

Ad-hoc network is an infrastructure less network which suits on-the-go deployment. Contrary to the traditional networks, there is no infrastructure such as centrally administered routers, servers or strict procedure for routing are involved in Ad-hoc networks. The nodes themselves are responsible for routing packets using some peer-to-peer routing procedure. In most of the cases, the devices used are power constrained and processing capability constrained. Moreover, the communication ranges of these devices are limited as well. With all this limitations, there are situations where adhoc network can only be used.

For instance, it is impossible to establish the wired network in the military missions because mostly it is performed unanticipated in the unknown territory. Likewise in military operations, the soldiers and the vehicles should communicate with each other. The soldiers might use handheld devices for communication and the communication devices may be integrated with the vehicle and other ammunitions. This is done to ensure the communication within the units while on-the-go, such a military situation results in frequently changing neighbors on whom a node relies for routing. This scenario therefore requires specially designed routing protocols to perform route discoveries in dynamically changing topology. Hence to suit such drasctically changing network, infrastructure less Ad-

Corresponding Author: Udhayan, J., PPG Institute of Technology, Faculty of Computer Science and Engineering, Anna University, Coimbatore Zone, India

hoc networks is effective than any other technology. Nevertheless the Ad-hoc networks should handle the nodes that drastically change its locations. Hence the routing protocols should be able to adapt to the dynamic node movements.

Unlike other networks the Mobile Adhoc Network (MANET) nodes are usually not familiar with the entire topology of their networks. Instead, they have to discover it every time before using the network. Therefore when a new node before entering into the adhoc network may announce its presence and should listen for announcements broadcast by its neighbors. This simple looking procedure is difficult to establish, therefore there are many routing protocols being used which can be classified as either proactive or reactive protocols.

The Table-driven (Pro-active) routing protocol maintains lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

- Sizeable amount of data maintenance for routing
- Slow reaction on restructuring and failures

Examples of pro-active algorithms are: Better Approach to Mobile Adhoc Networking (B.A.T.M.A.N), Optimized Link State Routing Protocol (OLSR).

In case of On Demand (Reactive) routing Protocol, a route on demand is discovered by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

- Induces increased routing load and delay
- Excessive route information flooding can lead to congestion

Examples of on demand algorithms are:

- Admission Control enabled on demand Routing (ACOR), Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Power-Aware DSR
- In roving military operations, the nodes are higly mobile. So it is difficult to maintain the list of neighbours and it requires quick restructuring. Therefore the routing protocols that suits the military mission is on-demand routing protocols

In reactive routing protocols, each node sends routing packets only on an arrival of a communication request. Most of the on-demand routing protocols follow the route discovering phase initially to search an efficient path to the destination node by broadcasting the route discovery packets into the network. This makes the reactive routing protocols more suitable for highly mobile and on-the-fly networks.

However the security of MANET protocols is always questionable, if used in highly mobile scenario such as military operations the demand on security is too high and there is no room for even a single security breach. Hence the MANET should include lightweight mechanism to perform security check other than implementing the complex security procedures.

2. PROBLEM DEFINITION

In highly roving operations like military mission, a single compromised node can cause various adverse effects. However implementing complex security procedures is not suitable due to high degree of mobility. Moreover the operation should be rough-and-ready because even a single link failure or compromise may result in severe consequences.

Moreover even the mostly used reactive routing protocol which adapts to the high degree of mobility is not even suitable to be used in military operation due to the varities of security threats. Various such security threats are discussed in the following section 3.

3. RELATED WORKS

The MANET if used in military operation will face serious of security threats. Few dangerous types of attacks are discussed below.

3.1. Security Breaches

Remote redirection attacks or otherwise called as black hole attack. In this kind of attack, a malicious node uses routing protocol to advertise itself as the shortest path to nodes whose packets it wants to intercept. Protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes towards a specific destination. In AODV, any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value.

A redirection attack is also possible in certain protocols, such as AODV, by modification of the hop count field in route discovery messages (Burmester and Medeiros, 2009). When routing decisions cannot be made by other metrics, AODV uses the hop count

field to determine a shortest path (Cordasco and Wetzel, 2009). In AODV, malicious nodes can attract route towards themselves by resetting the hop count field of the RREP to zero.

Once the malicious node has been able to insert itself between two communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop packets to perform a denial of service attack, or alternatively use its place on the route as a first step in man-in-the-middle attack.

Moreover generation of false routing messages is termed as fabrication messages (Lavanya *et al*., 2010). Such attacks are difficult to detect.

In routing table overflow attack, the attacker attempts to create route to non-existent nodes. The goal of the attacker is to create enough routers to prevent new routes from being created or overwhelm the protocol. Implementation and flush out legitimate routes from routing tables. Proactive routing algorithms attempt to discover routing information even before they are needed, while reactive algorithms create only when they are needed. This makes proactive algorithms more vulnerable to table overflow attacks.

The possible attacks by the external attackers are through injecting erroneous routing info, replaying old routing info or distorting routing info in order to partition a network or overloading a network with retransmissions and inefficient routing (Ahmad and Jabeen, 2011).

All this attacks exploits lack of authentication procedure and the integrity check procedure in the MANET routing protocols (Shi-Chang *et al*., 2010). Hence the secure routing concept had been introduced.

3.2. Secure Routing

No single standard protocol capture common security threats and provide guidelines to secure routing protocol (Kumar *et al*., 2010). Routers exchange network topology informally in order to establish routes between nodes. This feature is the primary target for various types of malicious attacks. In military operation, the detection of compromised nodes through routing information is difficult due to the dynamic topology of Adhoc networks. Moreover the Routing protocols for Adhoc networks must handle outdated routing information to accommodate dynamic changing topology. False routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there is sufficient number of valid nodes, the routing protocol should be able to bypass the compromised nodes. This however needs the existence of multiple, possibly disjoint routes between nodes (Lakshmi and AntonyKumar, 2010). Routing protocol should be able to make use of an alternate route if the existing one appears to have faulted.

4. EXISTING PROTOCOL

The protocol is in the process of being standardized at the IETF and currently AODV is an experimental RFC. Mobile ad hoc networks have typically been deployed on a small scale in controlled environments in various laboratories around the world. The AODV@IETF project aims to make available the first ever large-scale, publicly-usable ad hoc network using the AODV routing protocol. This network will allow an user to communicate not only with other users in the ad hoc network, but also with the hosts on the Internet, possibly over several wireless hops. The network has been designed to offer a seamless connection experience to the user. Therefore AODV is the widely used protocol designed to suit the Ad-hoc networks.

Dynamic Source Routing (DSR) is a routing protocol suitable for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

Authenticated Routing for Ad-hoc Networks (ARAN) detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN introduces authentication, message integrity and non-repudiation to an Ad-hoc environment. However it requires certain amount of security infrastructure. Moreover ARAN requires that the nodes should keep one routing table entry per source-destination pair that is currently active. This is certainly more costly than per-destination entries in non-secure ad hoc routing protocols.

There are various other routing and secure routing algorithms, however all those algorithms can’t detect and alert the mailcious entrant.

5. PROPOSED VIGILANT PROCEDURE

In a military organization the pre-deployed security infrastructure is not always possible. But the challenges are going to be too much more than the normal circumstances. Therefore the environment is classified in zones A, B, C.

In zone A-It is less adverse condition and the base is deployed where the deployment of ARAN like environment is possible.

In zone B-It is moderately adverse and the devices roves in expected fashion where implementation of ARAN is not possible however the secure zone is at the distance of few hops.

In zone C-The devices are at the adverse environment and the movement of devices is drastic, it may reach zone but only through considerable number of nodes.

As long as the devices are situation in zone A, it can implement more robust security measures but in zone B and zone C. Such measures are almost impossible to implement due to the uncertainty. Hence some simple mechanism, moreover in zone B and zone C it is adverse environment therefore the devices are more vulnerable towards verities of security breaches.

However implementing the complex encryption schemes are not possible with the Zone B and Zone C. Hence simple XOR and XNOR based encryption was proposed.

The XOR and XNOR operator is extremely common as a component in more complex ciphers. By itself, using a constant repeating key, a simple XOR cipher can trivially be broken using frequency analysis. If the content of any message can be guessed or otherwise known then the key can be revealed. Its primary merit is that it is simple to implement and that the XOR/ XNOR operation is computationally inexpensive. A simple repeating XOR/XNOR cipher is therefore sometimes used for hiding information in cases where no particular security is required.

If the key is random and is at least as long as the message, the XOR cipher is much more secure than when there is key repetition within a message. When the keystream is generated by a pseudo-random number generator, the result is a stream cipher. With a key that is truly random, the result is a one-time pad, which is unbreakable even in theory.

The device at zone B and zone C starts its journey from zone A. The authenticated devices thus have a secure secret key and nounce. Doesn't matter how secure the routing protocols are in an infrastructure less network, the attackers can enter into the network as legitimate nodes. There are many ways to perform secure routing but at the zone B and zone C it is not just about the secure routing but also about the capability to identify the illegitimate entities participating in the network and track and eliminating them is crucial. Hence the proposed work, implement a puzzle based autentication not at the routing level but send a broadcast geniune message which has the signature at one block and encrypted by the mixed XOR and XNOR algortithm. It may appear as if a military message and the received entities should respond to the message with their signature and in an encrpyted form. The entity does not responded and participated in the routing table can get busted.

Vigilant Algorithm

Step1: Trigger the vigilant Procedure
Step2: Send Message with signature encrypted using XOR or XNOR
Step3: At receivers end Identify the signature and send back the reply with its signature
Step4: Check for signature; absence of signature or wrong signature is the indication of the presence of the attacker.

Morever it is not proposed to add overhead to the routing protocols but to decouple from the routing protocols. Hence it does reduce delay in the routing as well as it improves energy conservation.

This simple authentication procedure can be initiated by the user himself which can be triggered to avoid being trapped. For instance, if a newly joined node proposes a shortest path before following the path, it can be tested using the vigilant procedure.

The AODV protocol consists of two phases: route discovery and route maintenance. An important feature of AODV for route maintenance is that it maintains timer-based state of every node. The routing table will expire if a route is rarely used. When the route expires, the route discovery is performed. Therefore a trigger can be set to initiate the vigilant procedure every time when the timer expires.

The vigilant procedure will alert the user with the malicious entrant, but with the other protocol either they try to avoid or else it itself becomes vulnerable to the attack.

6. EXPERIMENTAL RESULTS

Various protocols that are being used in Adhoc network are compared and the results are as follows **Table 1**.

Table 1. The comparison of various protocols

	Protocols			
Attacks	AODV	DSR	ARAN	Vigilant
Remote Redirection modification of hop count				
Sequence Number	Can't detect	Can withstand	Can withstand	Can detect
Source Route	Can't detect	Can withstand	Can withstand	Can detect
Tunnelling	Can withstand	Can withstand	Can withstand	Can detect
Spoofing	Can't detect	Can withstand	Possible but tedious	Can detect
Fabrication of Error msgs	Can't detect	Can withstand	Can withstand to some extent	Can withstand
Fabrication of	Can withstand	Can detect	Can withstand	Can detect
source routing and Cache Poisoning	Can't detect	Can detect	Can withstand	Can withstand

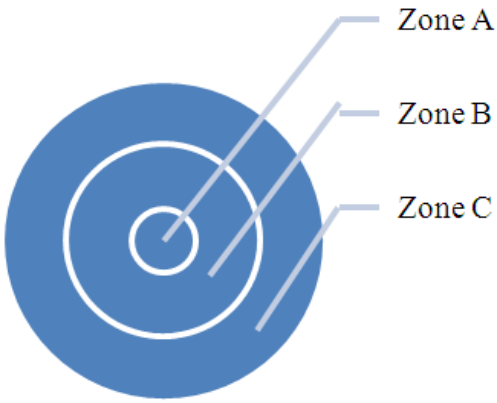

Fig. 1. Various zones in military mission

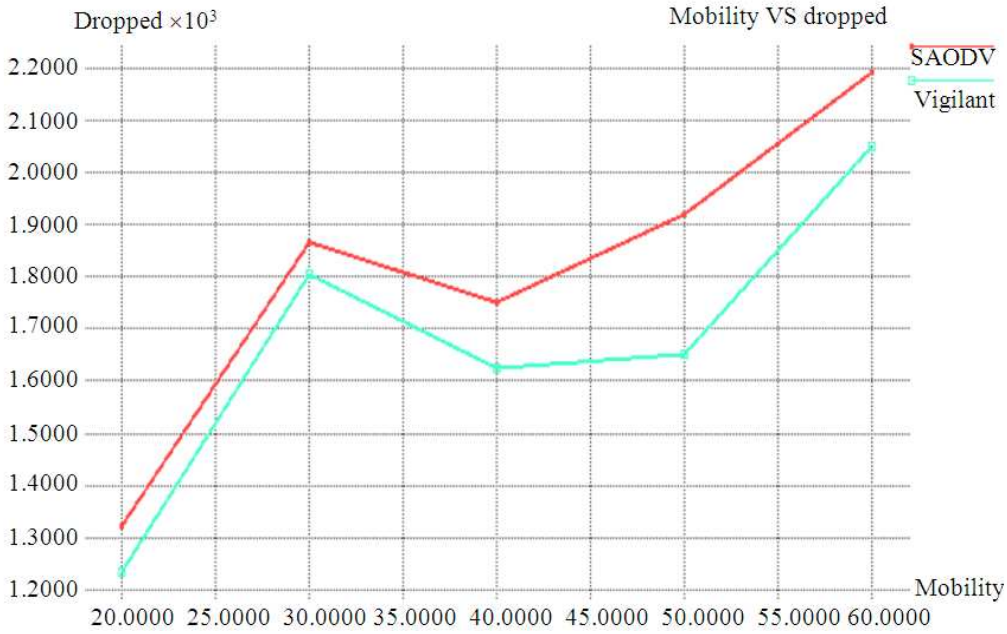

Fig. 2. Mobility Vs dropped packets

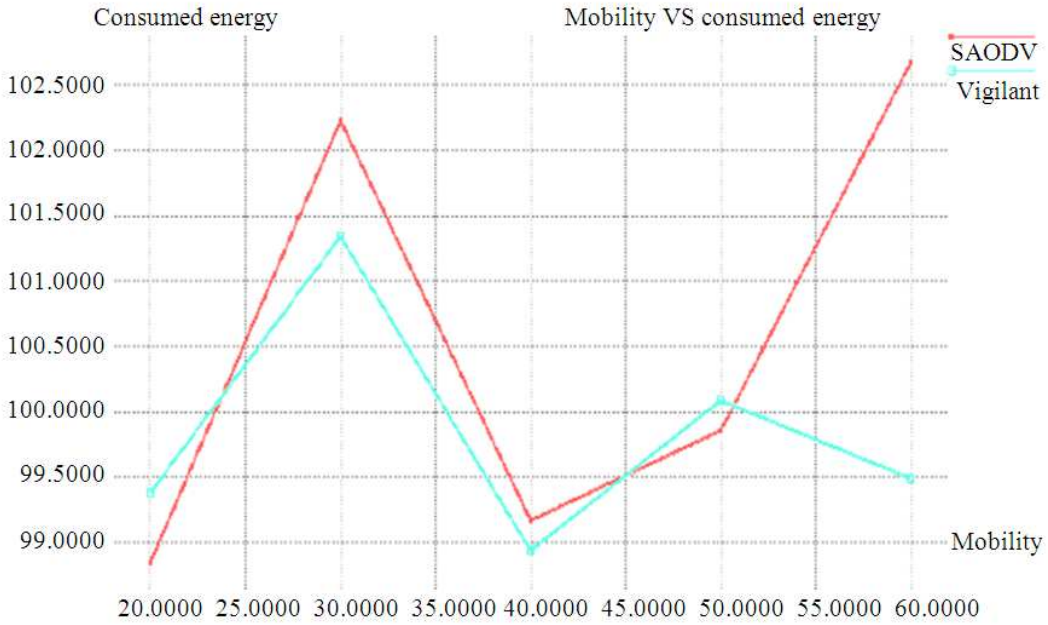

Fig. 3. Mobility Vs consumed energy

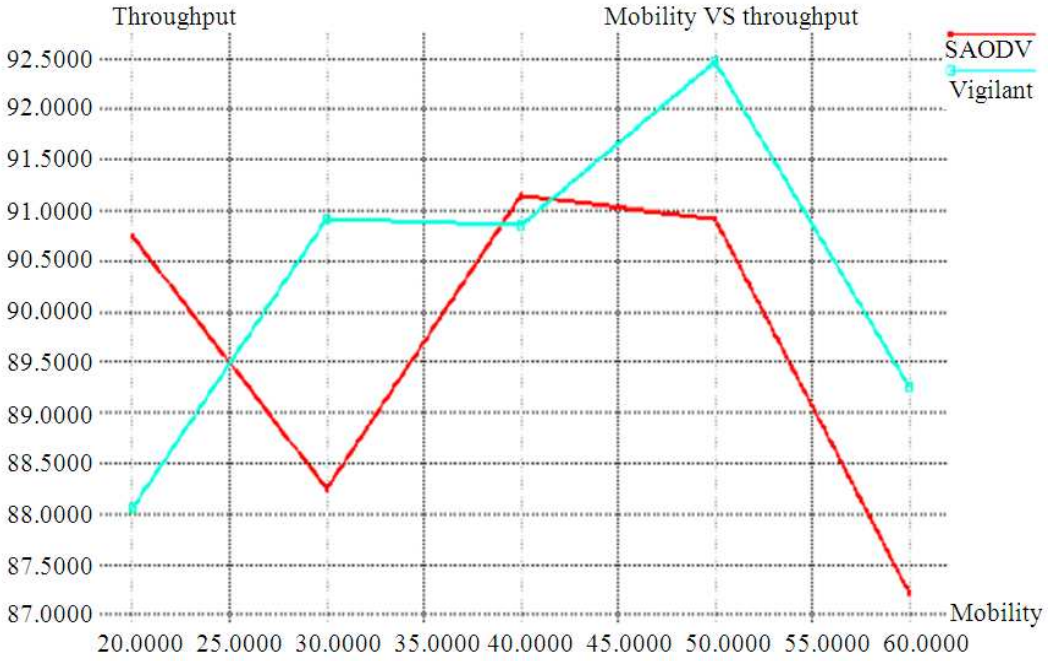

Fig. 4. Mobility Vs Throughput

DSR is a routing protocol, which explicitly states routes in data packets. These routes lack any integrity checks and a simple denial-of-service attack can be launched in DSR by altering the source routes in packet headers.

Modification to source routes in DSR may also include the introduction of loops in the specified path. Although DSR prevents looping during the route discovery process, there are insufficient safeguards to prevent the insertion of loops into a source route after a route has been salvaged.

AODV and DSR implement path maintenance measures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the node upstream of the link break broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. The vulnerability is that routing attacks can be launched by sending false route error messages. Suppose node S has a route to node X via nodes A, B and C. A malicious node M can launch a denial of service attack against X by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and X. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for X and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to X, M can successfully prevent communications between S and X.

The chance of detecting the attack is possible with the vigilant procedure but however failure to effectively applying the vigilant procedure can still leave the attacker undetected.

The Network Simulator NS2 had been used to evaluate the performance of vigilant algorithm. The AODV protocol which is available in the default installation of NS2 is used.

The following **Fig. 1-4** show that vigilant algorithm gives better results than secure AODV algorithm.

7. CONCLUSION

The Ad hoc network provides support to highly roving military operations, the protocol AODV adapts to its need. However the security is huge concern, implementing and using complex security mecanism for routing may not me possible in higly mobile and time critical operations. Hence in this work three possible military zones A, B and C identified based on the mobility and hostility. The Zone B and C are higly hostile and the mobile zones zone C brings the opportunity to implement secure routing and security measures. However implementing them in B & C brings delay and consumes more power this may even cause the time critical mission to fail. Hence a vigilant algorithm is proposed which utilizes the security at zone A and helps to identify the adverse entity in the routing zones. The vigilant algorithm is compared against the secure AODV algorithm and the result shows improved performance of vigilant algorithm.

8. REFERENCES

Ahmad, I. and H. Jabeen, 2011. Enhanced load balanced AODV routing protocol. Int. J. Comput. Sci. Inform. Security, 9: 98-101.

Burmester, M. and B. Medeiros, 2009. On the security of route discovery in MANETs. IEEE Trans. Mobile Comput., 8: 1180-1188. DOI: 10.1109/TMC.2009.13

Cordasco, J. and S. Wetzel, 2009. An attacker model for MANET routing security. Proceedings of the second ACM Conference on Wireless Network Security, (WNS '09), ACM Press, New York, USA., pp: 87-94. DOI: 10.1145/1514274.1514288

Kumar, J., M. Kulkarni and D. Gupta, 2010. Secure routing protocols in ad hoc networks: A review. Proceedings of the International IJCCT, (IIJCCT).

Lakshmi, P.R. and V. AntonyKumar, 2010. Security aware minimized dominating set based routing in MANET. Proceedings of the IEEE Second International Conference on Computing, Communication and Networking Technologies, Jul. 29-31, IEEE Xplore Press, Karur, pp: 1-5. DOI: 10.1109/ICCCNT.2010.5591709

Lavanya, G., C. Kumar and R.M.A. Raj, 2010. SECURED backup routing protocol for ad hoc networks. Proceedings of the IEEE International Conference on Signal Acquisition and Processing, Feb. 9-10, IEEE Xplore Press, Bangalore, pp: 45-50. DOI: 10.1109/ICSAP.2010.62

Shi-Chang, L., Y. Hao-Lan and Z. Qing-Sheng, 2010. Research on MANET security architecture design. International Conference on Signal Acquisition and Processing, Feb. 9-10, IEEE Xplore Press, Bangalore, pp: 90-93. DOI: 10.1109/ICSAP.2010.19