IMPACT: Journal of Research in Engineering and Technology (IMPACT: JIET)
Vol. 1, Issue 1, Jun 2017, 1-8

DEFENDING AGAINST PACKET DROPPING ATTACKS IN MANET: ENRICHED ACKNOWLEDGE SCHEME

A.PRIYADHARSHINI[1], R.THIYAGARAJAN[2], K. RAAGHUL[3], J. RANJITH[4] & S. PRIYADHARSHINI[5]

[1]Assistant Professor, Department of Computer Science and Engineering,
Knowledge Institute of Technology, Salem, Tamil Nadu, India

[2]Assistant Professor, Department of Electronics and Communication Engineering,
Shreenivasa Engineering College, Dharmapuri, Tamil Nadu, India

[3,4,5]Research Scholar, Department of Computer Science and Engineering,
Knowledge Institute of Technology, Salem, Tamil Nadu, India

ABSTRACT

Wireless network has led to highest popularity ever been anywhere. Although spaces during the attack on malicious node at a distant point in the re-location of the network node to another malicious packets and tunnels will hold them. Each network node and other nodes in MANETs presumably co-operate that the bad and non-cooperative nodes in the network to malicious attackers can be easily compromised by inserting MANETs. The traditional centralized monitor mechanism of dynamic topology structure which have no longer feasible MANETs. At this moment, it is safe for any malicious node packet from the source node to the destination node and the acknowledgement packet indicates that there will be ACK packet. The S-ACK introduces to view the group of three on each side along with the malicious node. After the missing packets of MRA, wrong test program verifies the information in a different way. The report has already targeted the malicious node the creates node for receiving packets or else it is a reliable misconduct and destination nodes are marked that the malicious nodes assign both sender and receiver side of the digital signature, but the use digital packets and packages to be forbid. Session key encryption technique reduce network overhead. It will increase the overhead of such networks while increasing the number of malicious node. Session key generator which requests a valid group signature that is dependent on request of main anchor forward. Collector session key generator generates the session key that request forward and maintains a session between the source and destination. At the time of transaction, session key generator will be expiring the session key or completely deactivate the nodes. Rijndael algorithm was developed for generating the session key and also from an original key Rijndael defines a method to create the series of sub keys. Input circuit sub-function is used to create keys and the input Rijndael 8-bit byte data blocks concluded

KEYWORDS: MANET, Session Key, Rijndeal Algorithm

INTRODUCTION

It can be configured by the network technician in MANETS mobile because they use wireless connections to connect to different networks. In that network as a cellular or satellite transmission which is a standard Wi-Fi connection. Some others are restricted to a local area wireless devices and internet MANETs connected. For example, a VANET (Vehicular Network Technology), road vehicles, communication equipment allows for a type of MANET. Automotive

Internet connection allows data to be sent over the Internet to a live Internet connection, wireless roadside equipment and vehicles. The data is used to measure and monitor traffic conditions, vehicle or truck fleets. Because of the dynamic nature of MANETs, they are usually quite safe so it is important to be aware of data that is sent is a MANET. A specific purpose of becoming a mobile cluster network is connected through a set of wireless links to mobile devices will become a self-configuring network that is available. The purposes including, but not an army in the field, such as a combat regiment should not be limited to the purpose of setting up a mobile network. The city and the need for constant communication buses picking up students from different parts of the sensor and also some of the data presented for the purpose of a central site.

It's Data Encryption Standard (DES) is that it supersedes. Federal information encryption standard Rijndael symmetric key algorithm used. Careful and detailed analysis of selected characteristics of the safety and effectiveness of the Rijndael algorithm. Therefore, the encryption or decryption heroes of a particular change in the volume of data (one round) (a round function) is accomplished through. Rijndael round function provides the details. Create a series of sub-keys from the original key Rijndael defines a method. Sub-function of the input circuit is used to generate keys. Rijndael, its safety, its cost and its algorithm and implementation, based on the characteristics of the assessment. Safety was the primary focus of the analysis is zero, but the Rijndael algorithm based on the selection and implementation of its simple properties. There were several candidate methods of analysis based on the Rijndael, because of security, performance, efficiency, ease of implementation and flexibility was selected as the best combination.

An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself. Accordingly, the study of the defense to such attacks should be explored as well. With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture [4].

In this paper, we have presented an optimization methodology allowing maximizing the efficiency of solar harvester for self-powered WSN devices have been proposed [6]. This methodology relies on com- pact models of both the PV module and the harvesting circuit, which implements an analog MPPT technique already proposed in the literature. The model of the PV module is discussed in detail, and a simplified parameter extraction procedure is proposed.

In this paper, we make two contributions to the area of secure routing protocols for ad hoc networks. First, we give a model for the types of attacks possible in such a system, and we describe several new attacks on ad hoc network routing protocols. Second, we present the design and performance evaluation of a new on-demand secure ad hoc network routing protocol, called Ariadne, that withstands node compromise and relies only on highly efficient symmetric cryptography[9]. In this paper, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to sup- port use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network [8].

RELATED WORK

Watchdog program and the limited transmission power and receiver collision TWOACK successfully solves the problems posed. However, the process of acknowledgment for each packet transmission process to include a significant amount of unnecessary network overhead. Due to the redundant transmission process MANET's and limited battery power, the nature of which can easily degrade the life of the entire network. ACK scheme, the period of time before receiving an acknowledgment packet source node to a destination node, it seems that there is no way that any malicious node receives the packet, send ACK packet is not safe. A group of three on each side with the aim to introducing the S-ACK mode of a malicious node want to be find the first node to the next node, the third node of a packet, the malicious MS ACK packet back to the second and third nodes, the node sends otherwise. MRA projects after missing packets incorrect test to verify that the original receiver that received the information in a different way. After the report has already been the target of malicious node creates a node that receives the packet. Otherwise, according to reliable misconduct and the destination node is marked as malicious. Both the sender and the receiver side to prevent the forging of digital packets of digital signatures, used to sign packages. Necessary resources and implementing digital signatures and RSA can be used for both digital signatures included.

Wireless networks for data communication between the different parties and allow them to maintain their mobility is its ability. However, this communication is only in the range of transmitters. Distance between two nodes that can communicate with each other at both ends when it crosses the border of their own means of communication.

The mobile technology, network mobile nodes that are equipped with both a wireless transmitter and a bidirectional wireless links, directly or indirectly communicate with each cut. Unfortunately MANET open and distance among the various types of arrangements are vulnerable to attacks. For example, the nodes' lack of physical protection, malicious attackers can easily capture and compromise to reach out to the edges. MANET if feasible and also because of the distributed architecture dynamic topology is no longer a traditional centralized final was MANETs. In such case, it is specially designed for MANET's an intrusion detection system (IDS) important to create.

PROPOSED WORK

In our proposed, a session key cryptography techniques that reduce the network overhead. Network overhead increases when number of malicious node in network increases because the count of acknowledged packet increases. The trusted anchor forwards the request to session key generator if the request contains a valid group key signature the session key generator generates a session key and forwards the session key to collector and to the requester to maintain a session between source and destination. If the transaction is completed by the time the session key has expired or to disable the session key generator. The session key is generated using the Rijndael algorithm. Rijndael also defines a method to generate a series of sub keys from the original key. Sub-function of the input circuit is used to generate keys. For input, Rijndael 8-bit byte data blocks that form a one-dimensional arrays accepts

The session manager module functions are

- Generate session key and store it in key store
- Disable session key

MODULE DESCRIPTION

The following modules are followed to implement the proposed scheme: ACK implementation, Secure Acknowledgment (S-ACK), Misbehavior Report Authentication (MRA), Digital Signature Validation, Session Key.

Ack Implementation

ACK is basically an end – to – end acknowledgment scheme. It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected. The basic flow is if Node A sends a packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A), if ACK from the destination get delayed then it S-ACK process will be initialized.

Secure Acknowledgment (s-Ack)

In the S-ACK principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

Misbehavior Report Authentication (MRA)

The MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

Digital Signature Validation

In all the three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

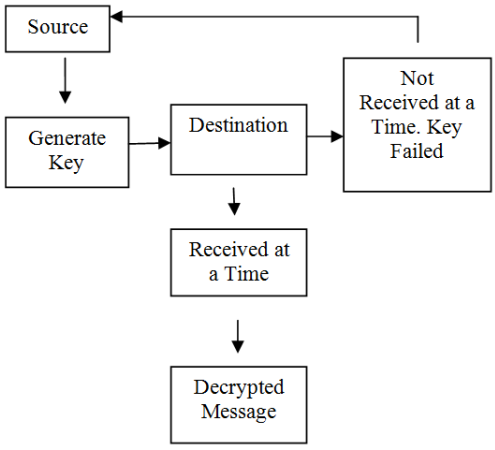

Figure 1: Digital Signature Validation

E SESSION KEY GENERATION

In this module, generate the keys for transfer the message from source node to destination node. After the session key will reached at out of time then the generated key will expired or discarded. Again it will generate the new keys it will transfer and reached within time after decrypt the messages.

ALGORITHM

There is an interactive cipher Rijndael cipher. It consists of a series of changes to hide or decipher data. Rijndael encryption and decryption of data volume of sub keys to enter the start and end of steps and additional step is performed as a protection against crypt-analyster. Rijndael a block of data hiding, leaving you in the first round itself into the mix, add a key step sequence (block a subkey XORing), then switch to regular rounds, then had to make a final round.

```
Rijndael(State,CipherKey) {
KeyExpansion(CipherKey,ExpandedKey);
AddRoundKey(State,ExpandedKey);
For (i=1 ; iFinalRound(State,ExpandedKey + Nb*Nr);
}
```

And the Round function is defined as:

```
Round(State,RoundKey) {
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,RoundKey);
}
```

RESULTS

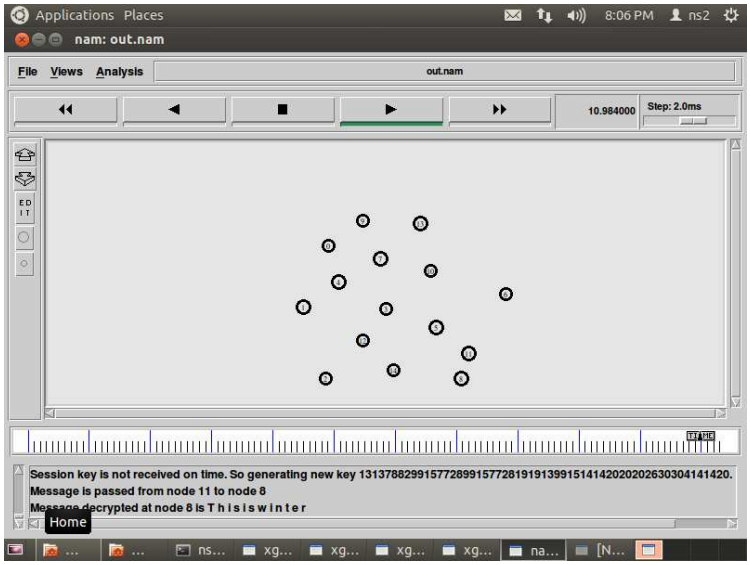

Figure 2: Key Not Received at Time

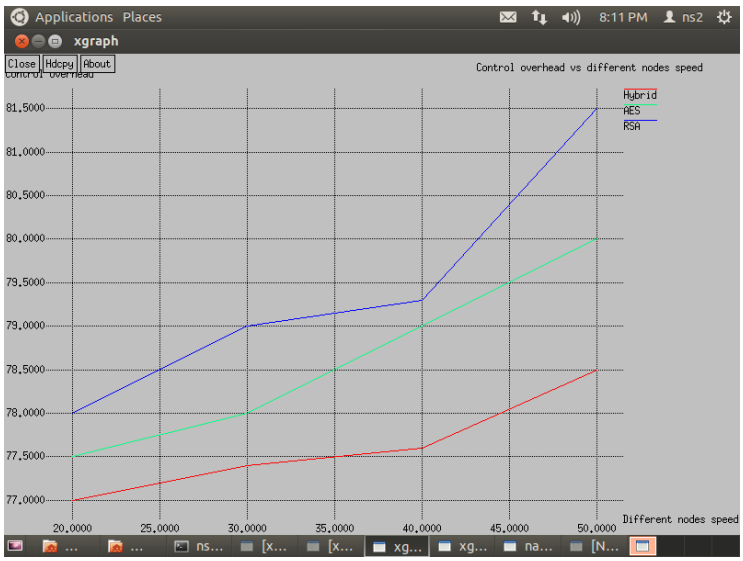

Figure 3: X Graph

CONCLUSIONS

Packet dropping attack has always been a major threat to security in MANETs. Well-known methods, especially for MANETs compared to the protocol designed by simulations in different situations EAACK, as opposed to the novel, IDS. Conflict, limited transmission power and abuse cases as a result of the monitoring receiver TWOACK report and demonstrate positive performances AACK. In this newly proposed scheme called EAACK and it provides better performances comparing to all other existing approaches. The EAACK scheme implements digital signature which causes network overhead which can be further reduced by hybrid key cryptography. This cryptography technique uses Rijndael algorithm for providing security and Zone Routing Protocol (ZRP) to find the route between source and destination. Future enhancement: Acknowledging the possibility, more complex encryption methods to reduce the network load caused by the digital signature, acknowledging the potential and to eliminate the need for review of the key exchange mechanisms to distribute keys

REFERENCES

1. K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, “Which wireless technology for industrial wireless sensor networks? The development of OCARI technol,”IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
2. R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” inLecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.
3. R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: A survey,” inProc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
4. T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” inWireless/Mobile Security. New York: SpringerVerlag, 2008.
5. L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
6. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, “Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks,”IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.
7. V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approach,”IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
8. Y. Hu, D. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” inProc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.
9. Y. Hu, A. Perrig, and D. Johnson, “ARIADNE: A secure on-demand routing protocol for ad hoc networks,” inProc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.
10. G. Jayakumar and G. Gopinath, “Ad hocmobile wireless networks routing protocol—A review,” J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.