Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp.4102-4108
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.422

A Hybrid Cryptography Approach To Safeguard The Privacy In A Manet

Devesh Pratap Singh Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002 devesh.geu@gmail.com

Vrince Vimal Department of Computer Science & Engineering, Graphic Era Hill University, Dehradun, Uttarakhand India, 248002 vvimal@gehu.ac.in

ABSTRACT

In a mobile ad hoc network (MANET), groups of mobile devices band together for a limited time to create a network that does not require any permanent infrastructure. Its use stems from the fact that it requires nothing in the way of upkeep or organization and can be moved from place to place thanks to wireless connections. The first is a decrease in network performance, and the second is a lack of security. Multiple attacks have hampered the efficiency of mobile ad hoc systems. For the sake of this article, we have limited our attention to network-layer active attacks. As a reactive routing system for ad hoc networks, Ad Hoc On-Demand Vector Routing protocol simply keeps routes between communicating nodes. AODV ensures that there are no routing loops even if a connection fails. Safe Ad-Hoc On-Demand Routers (SAODV) provides a trustworthy routing system for mobile ad-hoc networks. Our approach employs SAODV protocol and the Hybrid Cryptography Technique (DES, RSA Algorithms) on SAODV to boost performance and ensure confidentiality in MANET. This study provides a simulation-based comparison of the MANET routing protocols AODV and SAODV across a range of performance, energy, and packet-delivery metrics. The NS2 network simulation environment is used to realize the suggested cryptographic routing algorithm. As a result of implementing our proposed strategy, we see reduced energy consumption, a high packet delivery ratio, and a high throughput.

I. INTRODUCTION

Communication technology has advanced to new heights with the advent of the wireless ad hoc network. This is a relatively new invention for situations in which the administration of extensive infrastructure and its upkeep is a significant financial burden. Several performance and safety concerns have been raised about that. By its own nature, MANET is self-organizing, distributed, and capable of multi-hop routing, among other things. Due to the ad hoc nature of the network infrastructure and the inherent mobility of mobile

communication, topologies are established on the fly. Figure 1 depicts the MANET's underlying architecture.

MANET is susceptible to assault by bad actors. This highlights the importance of creating reliable intrusion- detection techniques for MANET security. We support the current trend of integrating MANETs into industrial settings as the technology improves to support this deployment. We strongly feel that addressing its possible security risks is essential for regulating to such a trend. In this research, we present Enhanced Adaptive Acknowledgement (EAACK), a new intrusion-detection system tailored to MANETs. EAACK relies on digital signatures to authenticate data packets by digitally signing the accompanying acknowledgement packet. The network's performance is not significantly impacted although EAACK's detection rates for malicious activities are higher than those of existing approaches under certain conditions. Author provides a safe method of communication that achieves excellent performance on the provided network. EAACK relies on a digital signature for authentication; however this adds network overheads that slow it down. Specifically, this research will present a Hybrid cryptographic technique with the goal of decreasing network overheads. The acknowledgement packet is not digitally signed when using the Hybrid Cryptographic Technique, but rather the data packet is encrypted with a strong key.

Nodes in mobile ad hoc networks engage in wireless communication with one another. Since the radio range in this network is so short, intermediate routers are used to facilitate communication between the nodes. Due to the uniformity of the network's nodes' capabilities, information may be transmitted, received, and redirected between them without any problems. Therefore, most malicious nodes first gain access to the network and then modify data in transit. In a mobile ad hoc network, an attack can be launched using the data retrieved from these passing packets. Even worse, it may lower the network's efficiency. To combat the increased network cost caused by the digital signature in the EAACK method, a suitable solution domain has been established.

II. LITERATURE SURVEY

Secure Data Aggregation and Verification (SDAV) were proposed by the **Ozdemir et al**. The authors choose to employ elliptic curve cryptography (ECC) because of its superiority over more conventional asymmetric methods in terms of both key size and computational and bandwidth requirements. Since the ECC allows just one sensor to calculate the signature, the base station may focus on verification. In SDAV, the aggregator takes in all of the encrypted information from its participants, decrypts it, takes an average, and sends that average back to the participants. Each node checks its reading against the group average, and if the difference is large enough, it sends the aggregator a partial signature it formed using the group key established before deployment. The entire signature is created and transmitted

by the aggregator to the base station. When deciding whether or not to accept a measurement, a Merkle hash tree is used to ensure the measurement's consistency. As the answer**, Adnan et al** proposed as the typical total averaging function. This defense works well against stealthy assaults. Since each node has its unique identify and shares a secret key with the CH, it is also secure against Sybille attacks. However, selective packet and replay attacks are possible vectors of attack for this method. A compromised aggregator has the ability to simply ignore data packets.

Jelena et al proposed an effective method of combining encrypted data. Data privacy and security are both protected by the proposed solution. An operation of additive homomorphism encryption was proposed by the authors. The concept is to employ modular addition instead of the XOR operation, which is typically used in stream ciphers. In the face of passive attacks, this method holds up well. There has been no thought given to protecting against actual attacks. As such, the proposed approach takes probabilities into account. Since the detected measure is hidden by the injected random value, cryptanalysis is made more difficult by this property. However, the greatest obstacle to decrypting encrypted data is the origin of this value. The **Chu et al** suggested a secure aggregate threshold in . For this protocol to work, a large number of nodes must submit identical data before the base station will accept the aggregate data. Key management, secure aggregation, and authentication are the protocol's three distinct phases. In the first stage, when the aggregator has exchanged keys with each member, the nodes broadcast a shared temporary group key to one another.

III. PROPOSED WORK

Our proposed method, a hybrid encryption scheme, is intended to reduce network overheads while simultaneously increasing data security. To take advantage of the benefits of both asymmetric and symmetric cryptography, a hybrid approach was developed. Quickness and safety are the respective definitions of these virtues. To that end, our proposed system

The data will be encrypted using RSA, an asymmetric cryptography method, and DES, a symmetric key cryptography method. You can learn about the suggested hybrid encryption technique by referring to the diagram in figure 8. The solution for safe data transfer over a mobile ad hoc network is implemented using the architecture described below. The conventional AODV method of route discovery is initially used. After verifying the found path, data is encrypted with the DES algorithm, and then the cypher text obtained from that is processed with the RSA algorithm. At this point, the data packages are ready to be sent over the network. The RSA encryption key is first used to decrypt the received data, and then the DES technique is used to decrypt the plaintext. At the receiving end, the original text is eventually reconstructed.

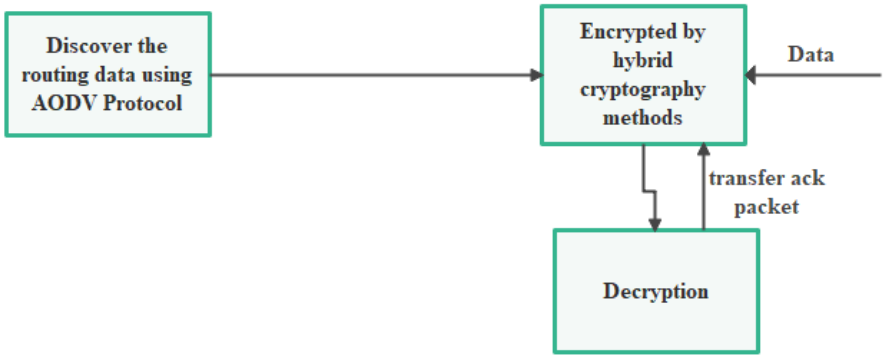

Fig 1: Block diagram of proposed framework

Figure 1, the block diagram of the proposed system, depicts the workflow of the procedures as follows for a clearer understanding of the proposed system:

a) Initially, using the AODV (Ad hoc On-demand Vector routing protocol) protocol to determine the path from origin to destination. Since the AODV routing protocol is a reactive routing system, routes are only calculated when they are actually used. In order to construct routes, AODV repeatedly queries nodes for their routes and then implements the ones that are requested.

b) The DES symmetric key algorithm and the RSA asymmetric key method are now invoked, respectively, to perform the symmetric and asymmetric cryptography, respectively, on the data. Information that needs to be transmitted may do it safely now. It's a cryptographic operation. There is now no risk to the confidentiality of the data being transmitted.

c) Using AODV to figure out the best path. After determining the best path, encrypted data is sent along it.

d) The data can be decrypted at the final destination node. The receiving node must confirm receipt of the data by sending an acknowledgment packet back to the sender.

e) By checking for an ACK packet, the source can verify that the correct node has received the data.

- ✓ **Hybrid cryptography framework**

This is how the Hybrid Encryption Technique is explained:

One extremely effective security approach is the Hybrid Cryptography Technique, which combines symmetric and asymmetric key cryptography. Assuming A is the sender and B is the recipient, the process goes as follows.

2) Using a common symmetric key cryptography algorithm, like DES, A's computer encrypts the plaintext (PT) from the plane. Creates an encrypted message with this method (CT). The key (K1) used in this transaction is a "one-time symmetric key" because it is only used once before being delete

Step 3: Using B's public key, A encrypts K1 using the one-time symmetric key she generated in Step 1. The term "key wrapping" is used to describe this transformation of a symmetric key.

Now, step 4 has A digitally enclose CT1, the cypher text, and the symmetric key's encrypted form, and send it to B.

Five, B gets the electronic package and opens it. B receives the encrypted cypher text (CT) and the one-time session key (K1) after opening the package (K2).

To retrieve the symmetric key (K1) that was encrypted with B's public key, B must now use the same asymmetric key methods as A and her private key (K3) (K2). Therefore, the final result is the unique symmetric key K1.

Seventh, to decipher the coded message, B uses the same symmetric key methods as A and the same symmetric key K1 (CT). The resulting unaltered text is the original (PT).

IV. RESLUTS AND DISCUSSION

Our simulations were built on top of ns-2 and included new features to account for mobile wireless networks. We have used the following simulation parameters to assess SAODV's performance:

Table1:Simulation paramters

Parameters	**Value**
Packet size	1024
Node size	70
Source node	23
Destination node	23
Idle power	0.0

As described above, we compared the energy, throughput, and packet-delivery ratios of black hole AODV and SAODV.

Energy: Given that many nodes fail owing to insufficient energy, power is crucial in an ad hoc network. Simulations were used to examine the energy behaviour of the various nodes.

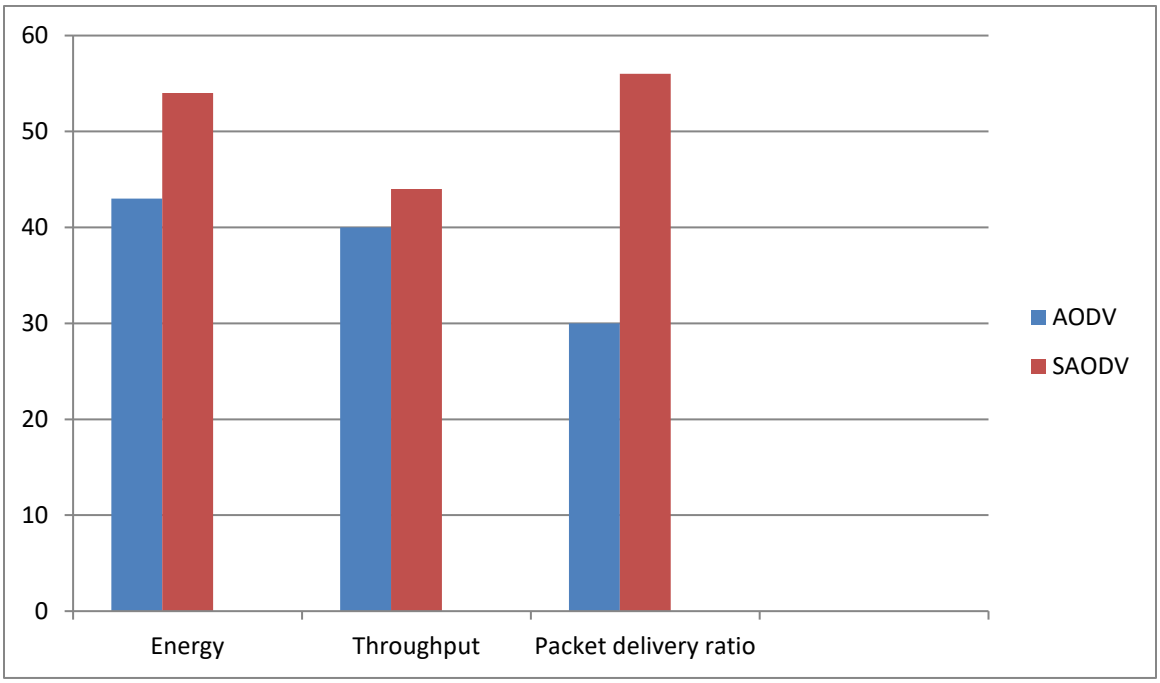

Fig 2: Comparing AODV vs SAODV Protocol

Throughput: When describing a communication channel, throughput is the typical rate of effective message delivery.

Packet delivery ratio: The rate at which "application layer" CBR sources generate packets in comparison to the rate at which the destination CBR sink receives such packets.

V. CONCLUSION

When it comes to protecting data in a mobile ad hoc network, a combination of the RSA and DSA algorithms is employed for encryption. For the purpose of keeping information safe while in transit, the AODV routing protocol makes use of that hybrid algorithm.

We use the NS2 network simulator to run the proposed encrypted routing algorithm. Further, the performance of the suggested routing technique is assessed and compared to the conventional secure routing methodology by using the trace files and awk scripts that are produced. Results from tests comparing the new model to the old one are summarised. Energy consumption is reduced, while the packet delivery ratio and throughput are both increased in our suggested method compared to the conventional one. The suggested framework is flexible enough to incorporate alternative secure routing methods. When combined with other safe routing methods, our suggested technique, the Hybrid Cryptography Technique, can improve network performance.

References

1. Jelena Misic, Vojislav Misic, Wireless personal area networks performance interconnections and security with IEEE 802.15.4., John Wiley & Sons Ltd, (2010).
2. Adnan Nadeem and Michael P. Howarth, A Survey of MANET Intrusion Detection and Prevention Approaches for Network Layer Attacks, IEEE Communications Surveys and Tutorials, vol. 15, no. 4, (2013).
3. S. Ozdemir and H. Ichakawa et al. (Eds.), Secure and reliable data aggregation for wireless sensor networks, LNCS 4836, pp. 102–109 (2010).
4. Z. Dawahdeh, N.S. Yaakob, A New Modification for Menezes-Vanstone Elliptic Curve Cryptosystem. Journal of Theoretical and Applied Information Technology, Vol. 85, pp. 290– 297 (2016).
5. M. Chu, H. Haussecker, and Zhao, Scalable information-driven sensor querying and routing farad ad hoc heterogeneous sensor networks, The International Journal of High Performance Computing Applications, Vol. 16(3), pp. 293–313 (2010).