International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802317

RC4 Algorithm Based Multi Path Encrypted Data Security Architecture for Mobile Ad-Hoc Network

Dr.N.Sureshkumar, P.Lokesh, M.Vijayakumar, S.Sarankumar

Muthayammal Engineering College, Rasipuram, Tamil Nadu, India

Department of Electronics and Communication Engineering, Muthayammal College of Engineering, Rasipuram, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Mobile ad hoc networks proved their efficiency in the deployment for different fields, but highly vulnerable to security attacks. It seems to be more challenging of in wireless networks. An ad hoc network is a group of wireless mobile computers (or nodes); in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. Existing research carried out provides authentication, confidentiality, availability, and secure routing and intrusion detection in ad hoc networks. Ad hoc network characteristics should be taken into consideration to design efficient data security along its path of transmission. The proposal of this work presented a Data Security Architecture (DSA) in improving the data transmission confidentiality in ad hoc networks based on multi-path routing. It utilizes the multiple paths between nodes in an ad hoc network to increase the confidentiality robustness of transmitted data. The original message to be secured is split into parts that are transmitted in multiple paths. The parted messages are encrypted on its course of transmission which improves the security to next level. Tree-based topology construct a tree structure for more efficient forwarding of packets to all the group members and with additional paths which can be used to forward packets when some of the links break.

KEYWORDS: Mobile ad hoc networks, security, Data SecurityArchitecture (DSA)

I. INTRODUCTION

Security is a critical issue in a mobile ad hoc network because the primary applications o f ad hoc networks are the military applications, such as the tactical communications in a battlefield, where the environment is hostile and the operation is security-sensitive. As compared with a fixed or a wired network, the characteristics of an ad hoc network pose many new challenges in security. For example, the wireless channels are more susceptible to various forms of attacks such as passive eavesdropping, active signal interference, and jamming. The co-operative nature of ad hoc protocols makes it more vulnerable to data tampering, impersonation, and denial of services. The lack of a fixed infrastructure restricts the applicability of some conventional security solutions, such as a Public Key Infrastructure (PKI), which relies on a centralized trust authority, and the intrusion detection system, which needs concentration point to collect audit data. The limited resources of mobile devices, such as the battery power, also limit the practical deployment of more comprehensive schemes in an ad hoc network. Finally, the continuous and unpredictable ad hoc mobility clouds the distinction between normalcy and anomaly, thus makes the detection of the malicious behavior difficult.

II. EXISTING SYSTEM

A few research works have been done to address the security issues in ad hoc networks. Security issues that have been addressed particularly for ad hoc networks include key management [1], secure routing protocols [2], handling node misbehavior [3], preventing traffic analysis, and so on [4]. In this paper, we address the data confidentiality service in an ad hoc network. The data confidentiality is the protection of data from passive attacks such as eavesdropping while they are transmitted across the network. The wireless channel in a hostile environment is vulnerable to various forms of attacks, particularly the eavesdropping. A more severe problem in a MANET is that mobile nodes might be compromised themselves (e.g., nodes be captured in a battle field scenario) and subsequently be used to intercept secret information relayed by them. In [5], we proposed a SPREAD (Secure Protocol for Reliable Data Delivery) scheme to statistically enhance the data confidentiality service in an ad hoc network. SPREAD is

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802317

based on secret sharing and multi-path routing. Multi-path routing has been extensively studied in a wired network context for aggregating bandwidth, reducing blocking probability, and increasing the fault tolerance, etc. [11]. However, the shared wireless channel has a significant impact on the performance of multi-path routing [9].

III. PROPOSED SYSTEM

The motivation of proposed data security in multi- path routing protocol is to divide the initial message into parts then to encrypt and combine these parts by pairs. Then use

the characteristic of existence of multiple paths between nodes in an ad hoc network to increase the robustness of confidentiality. This is achieved by sending encrypted combinations on the different existing paths between the sender and the receiver. In our solution, even if an attacker succeeds to have one part or more of transmitted parts, the probability that the original message can be reconstructed is low.

Scope of the project:

The purpose of this project is utilizes the multiple paths between nodes in an ad hoc network to increase the confidentiality robustness of transmitted data. The original message to be secured is split into parts that are transmitted in multiple paths. The parted messages are encrypted on its course of transmission which improves the security to next level in wireless networks.

Advantage:

1. Efficient forwarding of packets to all the group members.
2. Alternate path.
3. Additional paths which can be used to forward packets when some of the links break.

A. Multi path routing topology

The originality of the proposed approach is that it does not modify the existing lower layer protocols. The constraints applied in the security protocol are the sender `A' and the receiver `B' are authenticated, session key and message key is used for the encryption/decryption of frames at MAC layer and the authentication of the terminals, a mechanism of discovering the topology of the network is available, and the protocol uses a routing protocol supporting multi-path routing. Fig1 represent number of node creation for message transmission.

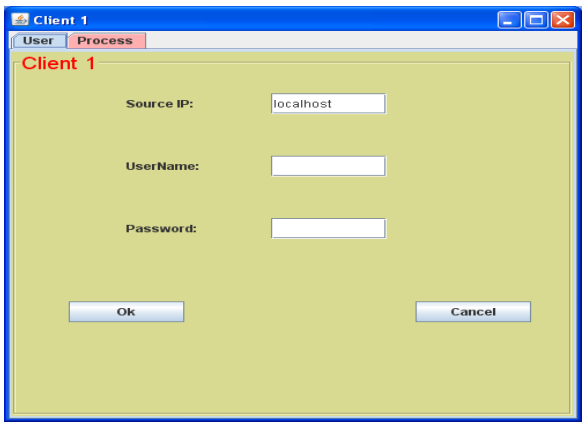

Fig 1: topology creation

B. Multiple path message Transmission

With the knowledge of network topology the proposed security model will use n routes (the message will be divided into n - 1 shares). One path is used for signaling, a second one is used to transmit in plain text a key share (randomly chosen) used to initiate the decombination process and the others (n -2 paths) transmit the different shares of the original message. Therefore the proposed data security multi-path protocol should have at least three links. Fig2 shows how the original messages split into various parts.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802317

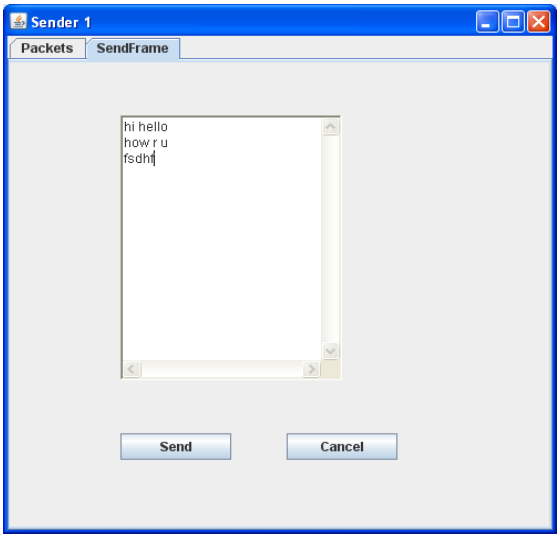

Fig 2: Message Transmission

C. Algorithm for Multi-path message transmission

RC4 Algorithm:

RC4 generates a pseudorandom stream of bits (a key stream). As with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way (since exclusive-or is a symmetric operation). (This is similar to the Vernam cipher except that generated pseudorandom bits, rather than a prepared stream, are used.) To generate the key stream, the cipher makes use of a secret internal state which consists of two parts:

1. A permutation of all 256 possible bytes (denoted "S" below).
2. Two 8-bit index-pointers (denoted "i" and "j").

The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA). Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

1. The key-scheduling algorithm (KSA):

The key-scheduling algorithm is used to initialize the permutation in the array "S". "key length" is defined as the number of bytes in the key and can be in the range $1 \leq$ key length ≤ 256, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.

2. Pseudo-Random Generation Algorithm (PRGA):

The PRGA modifies the state and outputs a byte of the key stream. In each iteration, the PRGA increments i, looks up the ith element of S, S[i], and adds that to j, exchanges the values of S[i] and S[j], and then uses the sum S[i] + S[j] (modulo 256) as an index to fetch a third element of S, (the key stream value K below) which is XORed with the next byte of the message to produce the next byte of either cipher text or plaintext. Each element of S is swapped with another element at least once every 256 iterations. Fig3 represent 256 random iteration of 8 bits and finally give the Original key value.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802317

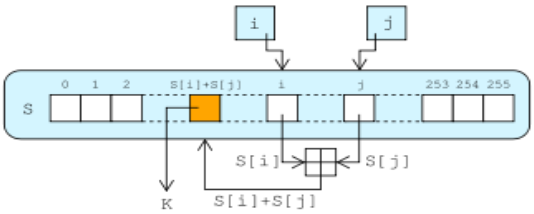

Fig 3: Pseudo-Random Generation

Algorithm Strengths:

1. The difficulty of knowing where any value in the table.
2. The difficulty of knowing which location in the table is used to select each value in the sequence.
3. a particular RC4 Algorithm key can be used only once
4. Encryption is about 10 times faster than DES.

IV. DATA SECURITY ARCHITECTURE (DSA)

Design an application layer situated on top of thenetwork (IP) layer that will manage the use of proposed two level data security solution to sent data securely. Specific header, called DSA header will be added for useful information to ensure security. DSA layer is situated between two important layers. The first one is the IP layer that will provide our protocol with important information about routing, number of available routes, quality of routes, depending on the routing protocol used. The second layer is the transport layer (TCP/UDP) that is able to manage retransmission, if needed, especially when topology has changed after the data transmission had started.

The Data Security Architecture introduces a set of features that can be incorporated with low overhead without modifying lower layer protocols. Both sender and receiver should implement DSA layer to be able to use this protocol. Before sending data between sender (A) and destination (B), the topology is provided in order to calculate the different routes n between A and B. If n is<3, a message error is generated, otherwise the n routes that will be used to transmit data securely will be chosen from the n existing
routes according to a cost function we will explain in detail in next section.

V. RESULT

The data security architecture presented in this work is tailored for on-demand multi-path data route, with encryption of parted messages in MANETs. This represents a better effort toward a formal security model that can deal with levels of security in safeguard the message being transmitted in ad hoc networks. Fig4 shows the receiver obtain the original massages in an ordered format.

Fig4: Receiving Messages

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802317

V. CONCLUSION

In the context of mobility, DSA requires that route discovery take place simultaneously with data communication. Consequently, in the proposed formal model, it prevents the adversarial nodes break up routes by inserting alternate path for the parted messages.

VI. FUTURE WORK

It prevents the original messages from sender to receiver by removing the all breakup internal nodes.

REFERENCES

1. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
2. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
3. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
4. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
5. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
6. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
7. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
8. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
9. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
10. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
11. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
12. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022