Secure Data Forwarding with Key Management in Vehicular Delay Tolerant Network

Seema Jangra[1,2], Amit Kant Pandit[1]

[1]Shri Mata Vaishno Devi University, Katra, J&K
[2]Indraprastha College for Women, Delhi University
Email: seema.mtech@gmail.com, amitkantpandit@gmail.com

Received: 15.07.2024 Revised: 13.08.2024 Accepted: 17.09.2024

ABSTRACT
A vehicle network with delay tolerance is called VDTN. In situations when a constant network connection cannot be ensured, this kind of network architecture is intended to facilitate communication between automobiles and other nodes. VDTNs solve the problems of sporadic connectivity and lengthy latency times by storing, transporting, and forwarding messages using the mobility of vehicles. Since vehicular delay-tolerant networks (VDTNs) operate in a unique context, they must overcome a number of security obstacles. Authentication and authorization, data integrity, confidentiality, privacy, secure routing, and trust management are a few of the major security issues facing VDTNs. The data integrity of the network's transit data must be preserved because to the limited resources in this advantageous environment. In order to provide privacy, secure routing, and handle malicious or self-serving nodes, data is sent to neighboring nodes based on trust. Cryptography techniques should also be used to encode the transit data. In order to maintain the security of transit data, we suggest a secure data forwarding technique in this study. The key management strategy used in this secure data forwarding system takes into account a dependable central authority for both key distribution and production. We are employing the symmetric cryptographic technique Advance Encryption Standard (AES) with a key management mechanism to accomplish an end-to-end data security strategy in VDTN. The suggested method involves the sharing of a private key amongst the trustworthy nodes in communication, with encrypted communications being routed to their target through opportunistic contacts.The suggested secure data forwarding scheme is examined using a few benchmark routing protocols according to different performance criteria. The research shows that the suggested approach can offer data security with outcomes that are similar to those of conventional data forwarding in VDTN.

Keywords: Vehicular Delay Tolerant Network, Symmetric Encryption, Advance Encryption Standard.

1. INTRODUCTION

A subset of delay-tolerant networks called automotive DTNs, or vehicular delay-tolerant networks, are made to manage communication in situations where conventional network infrastructure might be unreliable or unavailable. The capacity of these networks to store, transport, and forward data among a network of moving cars makes it possible to communicate in situations where continuous end-to-end connectivity is impractical. The poor density of vehicle nodes in VDTN causes frequent network partitioning due to sporadic opportunistic connectivity. In situations when traditional network infrastructure is unstable or unavailable, Vehicular Delay-Tolerant Networks (VDTNs) employ the "store-carry-forward" approach to manage sporadic connectivity and guarantee data delivery [1] [2].

Because of their dynamic topology, the communication links that are accessible during periods of intermittent connectivity are unstable and insecure. Monitoring vehicle node behavior or activity is necessary for dependable and secure communication in VDTN. With the exception of not having end-to-end connectivity, VDTN is subject to the same dangers, vulnerabilities, and assaults as other wireless networks [3]. Due to their basic decentralization, the VDTNs rely solely on node collaboration and bundle forwarding participation. But security of transit data is also crucial because of various misbehaving nodes, related attacks, and vulnerabilities [4].

The following factors must be taken into account when implementing VDTN and routing data: unauthorised access, data confidentiality, data integrity, and the detection of malfeasance or self-serving nodes [5]. The network's transit data must be protected because resources are few in the opportunistic environment. Data is sent to surrounding nodes based on their computed trust value in order to deal with selfish and disobedient nodes.

Transit data should be encoded using encryption techniques to improve data confidentiality and prevent integrity and unauthorised access attacks. Nevertheless, end-to-end secrecy is not provided by the bundle protocol in VDTN since confidentiality necessitates key management, a problem that still exists in VDTN. An end-to-end bundle authentication can be implemented to verify a bundle's integrity, which necessitates additional key management. In a situation like this, a centralised stationary node may be given control over key distribution and management.

2. LITERATURE REVIEW

The characteristics of a vehicular delay-tolerant network (VDTN) include varying latency, mobility-related broken links, and non-existent end-to-end connectivity. It is difficult to create routing protocols with the best possible routing performance because of its special qualities. In situations this difficult, trustworthy communication between various entities is vital.

The bundle protocol in the VDTN architecture defines the bundle (message) format. Using store-carry and forward approaches, the bundles are passed between various hosts that are in communication with one another. Bundle cached at intermediary nodes propagate based on either scheduled or opportunistic contact.

In bundle transmission, the links that are accessible are not secure because central authentication is not present. Data forwarding faces numerous security difficulties as a result of VDTN's unique features. With the exception of not having end-to-end communication, VDTN is subject to the same dangers, vulnerabilities, and assaults as other wireless networks. VDTNs are susceptible to attacks pertaining to availability, secrecy, and integrity because of their special features. The confidentiality, integrity, and various security concerns related to the bundle protocol in VDTN are listed in [6].

Achieving security objectives is hampered by the following VDTN features [7]:

- **Node and network heterogeneity:** There may be a variety of participating nodes to spread the data to the intended place because there isn't end-to-end connectivity. These nodes can be found in a variety of network types. Network heterogeneity leads to address and naming issues; authentication should be implemented.
- **Node's mobility:**Vehicle nodes are used in VDTN to transport and store the bundles. It is challenging to determine an end-to-end path between the source and the destination because of the high mobility and frequent network partitions.
- **High Delay:**Bundles are sent slowly as a result of network fragmentation and sporadic connectivity.

2.1 Attacks

In these kinds of networks, achieving the three security objectives of Confidentiality, Integrity, and Availability (CIA) is difficult. The VDTN is more susceptible due to the various risks and attacks that it faces. A VDTN environment can be vulnerable to a number of risks, including the existence of misbehaving or selfish nodes, resource consumption, denial of service, traffic storms, confidentiality and integrity issues, and ease of access. The various assaults that could occur in VDTN in response to these risks include denial of service (DOS) attacks, resource depletion, data injection and manipulation attacks, unauthorised access attacks, and attacks pertaining to confidentiality and integrity [8–10].

The implementation of VDTN and data routing should take into account the following factors, such as unauthorised access, data confidentiality and integrity, detection of misbehaviour, and selfish nodes, due to the existence of the risks and attacks previously described. DTNs are essentially decentralised networks that depend solely on nodes cooperating with one another and taking part in bundle forwarding. Network nodes occasionally exhibit selfishness or misbehaviour. Because the resource is limited, network security and privacy must be preserved by guarding against unwanted access.

In the DTN, maladaptive nodes can launch various assaults and lower network performance [10]. The following are some of the most frequent attacks that opportunistic networks and VDTN are vulnerable to:

Sybil: Any rogue node can appear as multiple identities when there is no central authority [11]. The malicious node in this kind of attack uses a lot of fake characters in order to get the most out of it or to transmit misleading information. The identity generation method and the way the system takes inputs from nodes without doing a trust evaluation are key components of a reputation system without a central authority. By taking advantage of this weakness, a Sybil attack can be carried out.

Black hole: A black hole attack is carried out by a maladaptive node that discards received messages rather than passing them to nearby nodes. The malicious nodes in this attack assert that they can deliver messages using the shortest path and consistently provide a good response even in the absence of route information to the intended destination. As a result, it allows a certain amount of messages to flow through before discarding them. The black hole attack is carried out via the black hole node. Using multiple copies based routing protocols, such as epidemic, in DTN provides inherent protection against black hole attacks. Since the message is present in several copies throughout the network, removing one copy won't have an impact on how well the network performs in comparison to other networks [12].

Message tampering: A malicious node has the ability to alter or temper the messages that are transmitted by the various nodes. When a routing activity is occurring between the source and destination nodes, the malicious node has the ability to tamper with the message [13].

Bad Mouthing: In order to damage the victim's reputation, the attackers in this attack decided to provide unfavourable reviews. The reputation of nodes with a high reputation is lowered by this malicious node [14].

Ballot Stuffing: Malicious nodes attempt to boost the reputation of peers with poor reputations in order to pack ballots [15].

On-Off attack: Because the rogue node has two personalities, it is difficult to identify this kind of assault. Malicious nodes, on the other hand, exhibit both good and poor behaviour to carry out this kind of assault. For the purpose of preserving their reputation, they offer both subpar and exceptional services. When they have different kinds of neighbours, they act differently [16].

Replay: The hostile nodes in this attack purposefully delay or repeat the communications. After a while, the adversary node deliberately forwards the message or retransmits it [17]. **Data analysis:** A malicious node seeks to collect information through a passive attack without interfering with normal network communication. An adversary conducting a data analysis assault continuously monitors network traffic in order to evaluate it and gather sensitive data. This kind of assault is challenging to detect since the message is tough to read and cannot be changed [18].

Unauthorized Access: Only authorised access may access the data transmitted over the network in order to protect privacy and confidentiality. Information privacy and integrity can be compromised by unauthorised access [19].

Denial of service: Malicious vehicle nodes bombard the target node with messages in an attempt to disrupt services and prevent it from performing the intended purpose. A denial of service attack occurs when an unscrupulous vehicular node floods the network with data packets. Distributed denial of service attacks of this kind can occur when multiple fraudulent vehicle nodes initiate the attack concurrently. This is the most prevalent and widespread assault that seeks to impair network functionality and interfere with services that are offered. [20].

Message delay: Malicious vehicle nodes add specific time slots to the message to postpone transmission after receiving it instead of forwarding it to the neighbours. As a result, when the message is needed, the honest vehicular nodes do not receive it [21].

Resource depletion: The vehicle network is particularly vulnerable to resource depletion attacks since the vehicular node has limited storage, processing power, and bandwidth. Resource depletion attacks can be carried out by any hostile vehicular node by unauthorised access, packet flooding, injecting spurious packets, vehicular node compromise, and data transmission by unauthorised apps [10].

Spamming: The attacker node generates and sends out a lot of spam messages to take up network bandwidth.

Table 2.1 categorises the aforementioned attacks into two groups: active attacks and passive attacks.

Table 2.1: Classification of Attacks

Active attacks	Passive Attacks
Sybil, Blackhole, Message tampering, Bad Mouthing, Denial of service, Message delay, Resource depletion, Ballot Stuffing, On-Off attack, Replay, Unauthorized Access, Spamming	Data analysis, Eavesdropping, Monitoring

Because VDTN lacks a central monitoring body and an encryption method, different attacks and unauthorised access may compromise the confidentiality and integrity of the network. Numerous distinct cryptographic techniques can be used to ensure the secrecy and integrity of data. The Rivest–Shamir–Adleman (RSA) algorithm, an asymmetric encryption technique, is used in [22] to achieve data confidentiality by presuming that the sender and recipient already know the keys. However, there is a pre-sharing of keys overhead. However, due to their computational cost (such as exponentiation in the case of RSA), asymmetric encryption algorithms are inefficient in VDTN routing, while symmetric encryption techniques are significantly quicker than their asymmetric counterparts [23]. In light of these findings, we have integrated symmetric cryptography methods into the data before using a key management strategy for forwarding.

DES (Data Standard Encryption) [24], [25], AES (Advanced Encryption Method) [26], [27], Blowfish [24], and other symmetric encryption algorithms are some of the frequently used ones. The most used symmetric encryption technique among them is AES, which has key sizes of 128, 192, and 256. Popular asymmetric key encryption techniques include the Diffie-Hellman algorithm [29], RSA (Rivest-Shamir-Adleman) [28], and others. The fact that asymmetric encryption is comparatively slower than symmetric encryption is one of the key distinctions between the two types of encryption algorithms. Symmetric cryptography is simple to build, quick to compute, and straightforward to implement. To improve the secrecy of transit data, a symmetric encryption technique with a suggested key management and distribution process is used in this research. Data is secured at the sender node using the Advance Encryption Standard (AES) to prevent unwanted access.

3. Secure trust-based data forwarding

Regarding VDTN data security issues, safe data forwarding is not provided by VDTN routing protocols. To ensure security, symmetric cryptography methods will be incorporated into these routing strategies. Since delivery delays have a significant impact on VDTN performance, we secure the data using a symmetric encryption technique. The distribution and administration of the key used in symmetric encryption presents the main obstacle. We have combined conventional routing with the symmetric encryption technique AES-128. But before any data is encrypted or decrypted in a vehicle, the sender and the recipient should agree on the same key. As a result, key distribution and management are important issues that need careful thought.

3.1 Key management and key distribution in VDTN

Sharing the encryption/decryption key is a difficult operation because of the moving cars and sporadic connection. In this study, we offer a key distribution and manufacturing approach that takes into account a dependable central authority. Key distribution and management are handled by the roadside unit (RSU), or central authority. The 128-bit key is generated by the roadside unit, which then distributes it to the car nodes within communication range according to their membership in the node and trust value.

Proposed key management process

Based on trust, the vehicle nodes are divided into two groups: the unsociable group and the social skeleton group. For the network to function better, members of the same groups should be in communication with one another. After identifying themselves using the lookup table they obtained from the RSU, the members of the social skeleton group converse with one another.

Prior to data transfer, data encryption is used in social skeleton communication. The source vehicular node (Vs) encrypts the data using the private key; the destination vehicular node (VD) shall decrypt the data using the same private key. The following procedures outline the suggested key distribution and management strategy:

The roadside unit keeps track of and refreshes the look-up table's list of vehicle nodes along with their membership values. When summary vectors from nearby vehicular nodes with varying membership parameter values are received, the look-up table is updated.

1. Vehicular nodes are classified into social skeleton groups and unsociable groups based on the total trust value.
2. The roadside unit uses a random number generator function once to generate a 128-bit key (simulation time taken into account).
3. The generated key is given to the vehicle nodes that are part of the social skeleton group and have a trust value.
4. Since members of the social skeleton group do not transfer data to the unsociable group, the key is not given to them.
5. To protect the data, every vehicle node in the social skeleton group uses the same encryption and group key for decryption.

The AES-128 symmetric key technique is employed in the process of safe data forwarding using the suggested centralised key management scheme. The encrypted text is sent to the member of the social skeleton group via any conventional routing systems after the payload appended to the bundle is encrypted using an AES encryption algorithm with a 128-bit key at the source end. Using the same 128-bit key, the encrypted bundle is received at the target end and decrypted.

3.2 Proposed Advance Encryption Standard (AES)

The Rijndael algorithm is another name for the AES encryption technique. The data block size of this block cypher is 128 bits. For a 128-bit key size, the AES algorithm employs 10 rounds, with the number of rounds varying according to the critical size.
Each encryption round consists of following main steps [30]:

1. Initialization:
   Input: Plaintext, Encryption Key
   Output: Ciphertext
   Initialize a dynamic S-Box based on the encryption key.
2. Key Scheduling:
   Generate a series of round keys using a complex key scheduling algorithm.
   Ensure each round key is unique and non-repetitive.
3. Encryption Rounds:
   For each round (up to N rounds, where N is adaptable based on input size or security requirements):
   a. Byte Substitution:
   Use the dynamic S-Box to substitute each byte of the input block.
   b. Mixing Rows and Columns:
   Perform a transformation that mixes both rows and columns. This can be achieved by rotating rows and shuffling columns.
   c. Key-Dependent Permutations:
   Apply permutations to the block based on the current round key.
   d. Non-Linear Transformations:
   Introduce non-linear operations such as XOR with round-dependent values.
   e. Include Round Key:
   XOR the current block with the round key.
   f. Introduce Randomness:
   Inject randomness at specific points.
4. Final Round:
   After completing all rounds, perform an additional round of transformations to ensure complete diffusion.
5. Error Correction Layer:
   Optionally, apply an error correction code to the output to protect against data corruption.
6. Output:
   The final transformed block is the ciphertext.
   The following rounds make up the decryption process:
7. Initialization:
   Input: Ciphertext, Encryption Key
   Output: Plaintext
   Initialize a dynamic S-Box based on the encryption key, matching the one used during encryption.
8. Key Scheduling:
   Generate the same series of round keys used in encryption using the complex key scheduling algorithm.
   Ensure that each round key matches the corresponding key in the encryption process.
9. Decryption Rounds:
   For each round in reverse order (from N to 1):
10. a. Remove Round Key:
   XOR the current block with the round key used in the corresponding encryption round.
   b. Inverse Non-Linear Transformations:
   Apply the inverse of the non-linear operations that were performed during encryption.
   c. Inverse Key-Dependent Permutations:
   Reverse the permutations applied during encryption based on the current round key.
   d. Unmix Rows and Columns:
   Reverse the mixing of rows and columns.
   e. Inverse Byte Substitution:
   Use the inverse of the dynamic S-Box to substitute each byte back to its original value.
11. Final Reverse Transformation:

After completing all rounds, perform the inverse of any additional transformations applied during the final encryption round.

12. Error Correction Layer:
    Optionally, use the error correction code to verify and correct any errors in the decrypted output.
    Output:
    The final transformed block is the plaintext.

Table 3.1: Features of the AES Symmetric Key Encryption Algorithm

AES-128 Characteristics	
Block Size	128 bits
No of rounds	11
Key Size	128 bits
No of subkey in each round	5
No of subkey used in the pre-round calculation	5
Total no of subkeys used	10*5+5=55
Size of each subkey	32 bits
Size of Cipher Text	128 bits

AES is used to obtain the plain text with a block size of 128 bits. There will be ten rounds for AES 128. A different 128-bit subkey is utilised in each round. There are 128 bits in the master key.

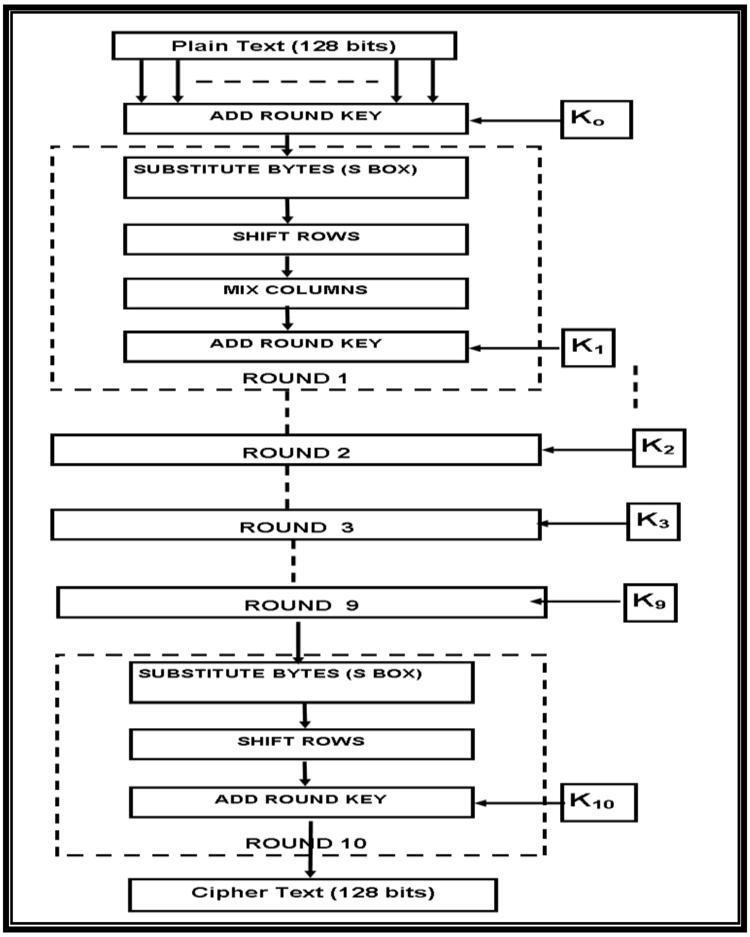


Figure 3.1: AES Encryption Process [30]

3.3 VDTN secure data forwarding

1. The payload of a message (M) created by the source vehicular node (S) is 512 bytes.
2. The message (M) (m) is composed of blocks, each of 128 bits.

$$M = \sum_{i=1}^{n} m_i \tag{3.1}$$

where the values of n, the number of blocks, and mi, a block of 128 bits, are determined by the bit count of message M.

3. The roadside unit uses a random function of size 128 bits to generate a random key (K) when an opportunistic connection is made, and then uses a look-up table to distribute it among the social skeleton group members.

4. Figure 5.1 shows how each message block (mi) at the source node (S) is encrypted using the AES encryption process.

$$M_{E.T} = AES(m_i, K) \tag{3.2}$$

5. Encrypted message $M_{E.T}$ is transmitted via clever VDTN connections to the neighbouring nodes of the same group.

6. Encrypted message from source (S) to destination (D) $M_{E.T}$ is transmitted through routing protocols incorporated in a trust-based social skeleton strategy.

7. The encrypted communication is decrypted at the destination node (D) with the same key.

4. Implementation and Simulation setup

Table 4.1 shows the values for the ONE simulation parameters. With the deployment of 213 nodes, the simulation employed both the map-based and map-route movement models. The performance of the proposed secure data forwarding using key management approach was examined using various performance metrics, including packet delivery ratio, average latency, and overhead ratio. The analysis of the proposed method made use of existing benchmark routing protocols embedded with the proposed trust based social skeleton data forwarding.

4.1 Performance Evaluation

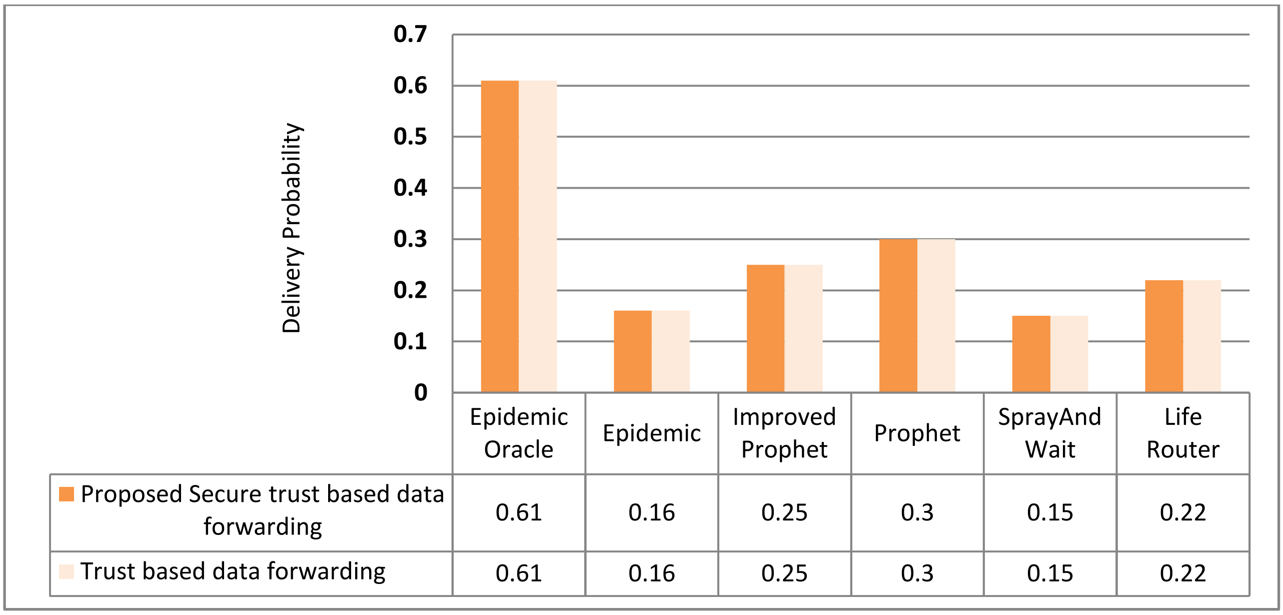
The performance of the VDTN is examined in relation to the suggested key management with ecryption technique. The results show that the suggested secure data forwarding strategy has a minor increase in delivery delay (Latency Average) but no influence on delivery rate or overhead ratio. The secure data forwarding method is compared to trust-based social skeleton data forwarding that does not use encryption or decryption in order to perform a comparative analysis. The benchmark routing techniques that are being evaluated are spray and wait, prophet, and epidemic.

Table 4.1: Simulation Parameters

Parameters	**Value**
Simulation Time	22600s
Interface	Bluetooth and High-speed interface
No of host groups	19
Number of Nodes	215
Routing Protocols	Epidemic, PRoPHET, Improved PRoPHET, Life Router
Movement Model	Map Route Movement ,MapBasedMovement
Speed of Mobile Nodes	0.3-1.6 m/s for pedestrians 2.8-13.10 m/s for cars
Buffer Size	For stationary node: 1.1 GB For mobile nodes: 5.5 MB
Size of Message	450KB -1.1 KB
Time to live (TTL)	800 min
Event Generator used	Message Event Generator
Transmission range	Bluetooth: 10m High Speed Interface = 500m
Transmission speed	Bluetooth = 250kBps High Speed Interface = 10MBps
World Size	100000 X 100000-meter square
Payload. enabled	True
Payload. size	514MB
Payload. Encryption. enabled	True
Payload. Encryption. algorithm	AES

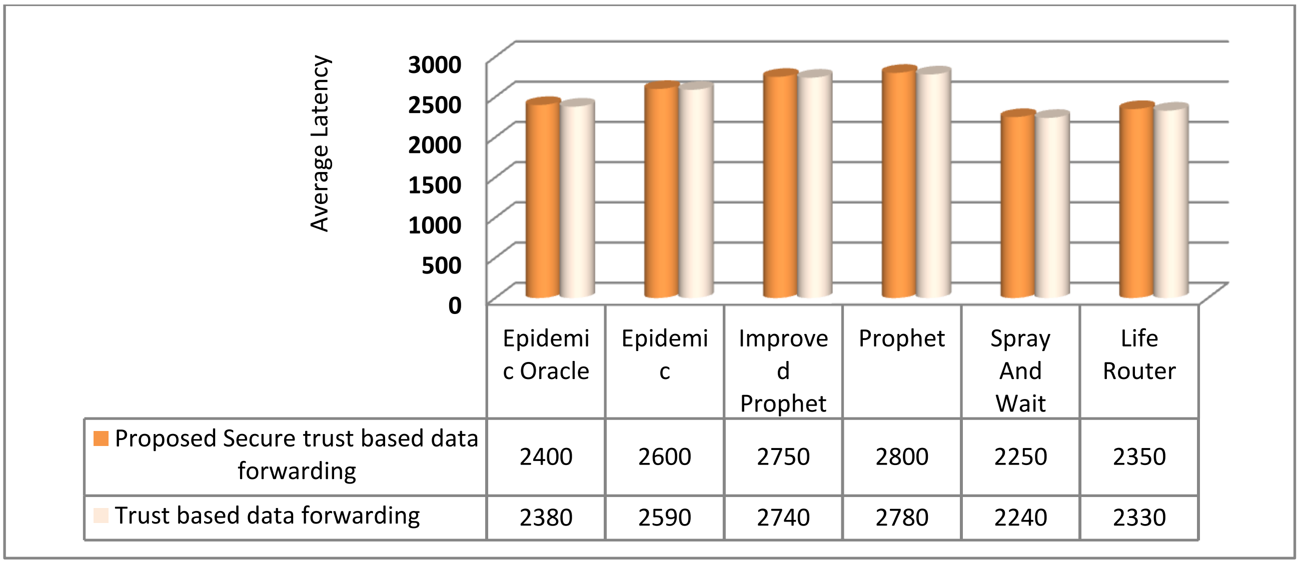
Table 4.1 displays the simulation parameters that were employed. A map-based movement model with synthetic traces is employed, with a 5MB buffer capacity, a 1 KB message size, and a 900 TTL (threshold values derived via simulation). The outcomes are derived from comprehensive simulations and juxtaposed with the outcomes of data transmission that is based on trust. Figures 4.1, 4.2, and 4.3 display the delivery probability, average delay, and overhead ratio of secure data transmission, respectively.

The results show that employing centralised key management techniques with encryption algorithms improves the confidentiality of the transit data while having no influence on the VDTN's performance. The dependable roadside unit, or fixed node, distributes the keys to the trustworthy members of the social skeleton exclusively.



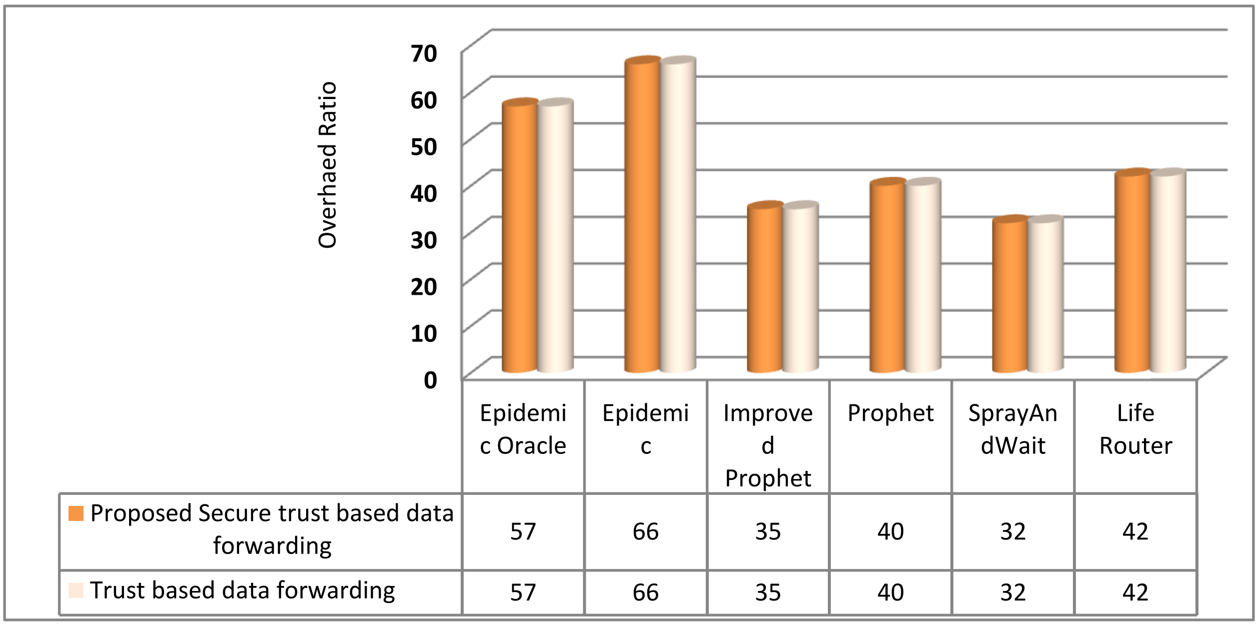
	Epidemic Oracle	Epidemic	Improved Prophet	Prophet	SprayAnd Wait	Life Router
🟧 Proposed Secure trust based data forwarding	0.61	0.16	0.25	0.3	0.15	0.22
⬜ Trust based data forwarding	0.61	0.16	0.25	0.3	0.15	0.22

Figure 4.1: Delivery Probability in Various Routing Protocols (trust-based social skeleton data transfer versus secure trust-based data forwarding)



	Epidemic Oracle	Epidemic	Improved Prophet	Prophet	Spray And Wait	Life Router
🟧 Proposed Secure trust based data forwarding	2400	2600	2750	2800	2250	2350
⬜ Trust based data forwarding	2380	2590	2740	2780	2240	2330

Figure 4.2: Average Latency (trust-based social skeleton data forwarding versus secure trust-based data forwarding)



	Epidemic Oracle	Epidemic	Improved Prophet	Prophet	SprayAndWait	Life Router
🟧 Proposed Secure trust based data forwarding	57	66	35	40	32	42
⬜ Trust based data forwarding	57	66	35	40	32	42

Figure 4.3: Overhead Ratio (trust-based social skeleton data forwarding versus secure trust-based data forwarding technique)

5. CONCLUSIONS

Because vehicular nodes are mobile and topologies change often, any rogue node can access the transit data as it is being transmitted. An encryption method is necessary to preserve the data's integrity and secrecy. But key management is required for the encryption and decryption processes, and this is a difficult task in VDTN. Key distribution and management are challenging given the lack of centralised monitoring authority and end-to-end connectivity. The stationary roadside unit is responsible for managing and distributing keys in the current work. The stationary node distributes keys based on the trust value of the node. Private key Advance Encryption Standard (AES) is used to improve the secrecy of transit data. The groups at the node receive the key from the roadside unit.

As compared to data forwarding in a trust-based social skeleton strategy, the simulation results demonstrate that encryption/decryption with key management approach improves the secrecy of transit data while retaining the same delivery rate and overhead ratio but slightly increases delivery delay. The amount of overhead incurred by the encryption/decryption process and the quantity of packets transmitted stay unchanged.

REFERENCES

[1] Rehman, G.U.; Zubair, M.; Qasim, I.; Badshah, A.; Mahmood, Z.; Aslam, M.; Jilani, S.F. EMS: Efficient Monitoring System to Detect Non-Cooperative Nodes in IoT-Based Vehicular Delay Tolerant Networks (VDTNs). Sensors 2023, 23, 99.

[2] S. Cc, V. Raychoudhury, G. Marfia, and A. Singla, "A survey of routing and data dissemination in DelayTolerantNetworks,"JournalofNetworkand ComputerApplications,vol.67,pp.128–146,2016.

[3] Feng Li, Yali Si, Ning Lu, Zhen Chen, and Limin Shen, "A Security and Efficient Routing Scheme withMisbehavior Detection in Delay-Tolerant Networks," Security and Communication Networks, vol. 2017,Article ID2761486,16pages,2017.

[4] Wu, Y.,Zhao, Y.,Riguidel, M.,Wang, G.,andYi, P.(2015), Securityandtrustmanagementinopportunistic networks:a survey.SecurityComm.Networks,8,1812–1827.

[5] Rehman, G.U.; Haq, M.I.U.; Zubair, M.; Mahmood, Z.; Singh, M.; Singh, D. Misbehavior of nodes in IoT based vehicular delay tolerant networks VDTNs. Multimed. Tools Appl. 2022, 1–19.

[6] S. Symington, S. Farrell, H. Weiss, P. Lovell, "Bundle Security Protocol Specification," draft-irtf- dtnrg-bundle-security-07.txt, work-in-progress, March 2009.

[7] Z. Zhang, "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges," Communications Surveys Tutorials, IEEE, vol. 8, no. 1, pp. 24 –37, quarter 2006.

[8] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, P. Yi, “Security and trust management in opportunistic networks: a survey,” Security Comm. Networks, vol. 8, pp. 1812–1827, 2015.

[9] Kumar Pramanik, K. ., B. Rahane, S. ., Jayamani, V. N. ., Mehra, R. ., C. R., M. ., & V. Athawale, S. . (2023). Cloud Computing based Wireless Sensor Network in Data Transmission With Routing Analysis Protocol and Deep Learning Technique. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 165–169.

[10] F. C. Choo, M. C. Chan, E.-C. Chang, “Robustness of DTN against routing attacks,” 2nd International Conference on Communication Systems and Networks (COMSNETS), pp. 1–10, Jan. 2010.

[11] J. Douceur, “The sybil attack,” 1st International Workshop on Peer-to-Peer Systems, pp. 251-260, 2002.

[12] B. Cherkaoui, A. Beni-Hssane, M. Erritali, “Quality control chart for detecting the black hole attack in vehicular ad-hoc networks,” Procedia Computer Science, vol. 113, pp. 170-177, 2017.

[13] M. S. Obaidat, I. Woungang, S. K. Dhurandher and V. Koo, “Preventing packet dropping and message tampering attacks on AODV-based Mobile Ad Hoc Networks,” International Conference on Computer, Information and Telecommunication Systems (CITS), Amman, 2012, pp.1-5, 2012.

[14] Z. Bankovic, J.C Vallejo, D. Fraga, J.M. Moya, “Detecting bad-mouthing attacks on reputation systems using self-organizing maps,” Computational Intelligence in Security for Information Systems, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, vol. 6694, pp. 9-16, 2011.

[15] I. Chen, F. Bao, M. Chang and J. Cho, “Dynamic trust management for delay tolerant networks and its application to secure routing,” in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.5, pp.1200-1210, May 2014.

[16] J. Caminha, A. Perkusich,M. Perkusich, “A smart trust management method to detect on-off attacks in the internet of things,” Security and Communication Networks, Article ID 6063456, 10 pages, 2018.

[17] B. G. Premasudha, V. R. Ram, J. Miller, and R. Suma, “A review of security threats, solutions and trust management in VANETs,” International Journal Next-Generat. Comput., vol. 7, no. 1, pp. 38–57, 2016.

[18] A. Dua, N. Kumar, and S. Bawa, “A systematic review on routing protocols for vehicular ad hoc networks,” Vehicular Commun., vol. 1, no. 1, pp. 33–52, 2014.

[19] R. Abassi, “VANET security and forensics: Challenges and opportunities,” WIREs Forensic Sci., vol. 1, pp. 1324, 2019

[20] P. Asuquo, H. Cruickshank, Z. Sun and G. Chandrasekaran, “Analysis of DoS attacks in delay tolerant networks for emergency evacuation,” 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, pp. 228-233, 2015.

[21] I. A. Sumra, J. AbManan, H.Hasbullah, “Timing attack in vehicular network,” Recent Researches in Computer Science, pp. 151-155, 2011.

[22] C. C. Sobin, Ct. Labeeba, K. D. Chandran,“An Efficient method for secure routing in delay tolerant networks,” Procedia Computer Science, vol. 143, pp. 820-826, 2018.

[23] Chandra, S. Paira, S. Alam, Sk. Bhattacharyya, Siddhartha, “A comparative survey of symmetric and asymmetric key cryptography,” International Conference on Electronics, Communication and Computational Engineering, ICECCE 2014.

[24] T. Nie, T. Zhang, “A study of DES and blowfish encryption algorithm,” Proceedings of 10th IEEE Region Annual International Conference TENCON, pp.1–4, 2009.

[25] M. E. Smid, D. K. Branstad, “Data encryption standard: past and future,” Proceedings of the IEEE, vol. 76, no. 5, pp. 550–559, 1988.

[26] J. Daemen, V. Rijmen, K. U. Leuven, “AES Proposal: Rijndael,” NIST, National Institute of Standards, 1999.

[27] N. I. of Standards-(NIST), “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication197, 2001.

[28] S. Burnett and S. Paine, “RSA Security’s Official Guide to Cryptography,” McGraw-Hill, 2001.

[29] A. Escala, G. Herold, C. Rafols, “An algebraic framework for Diffie - Hellman assumptions,” Journal of Cryptology, 2015.

[30] A. K. Mishra, N. Tripathi, M. Vaqur and S. Sharma, "Artificial Intelligence based Security Solution for Data Encryption using AES Algorithm," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 1685-1690, doi: 10.1109/ICSCDS56580.2023.10104702.