IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 17, 2018, accepted August 19, 2018, date of publication August 22, 2018, date of current version September 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2866759

Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication

GULSHAN KUMAR[1], (Member, IEEE), RAHUL SAHA[1], (Member, IEEE), MRITUNJAY KUMAR RAI[2], AND TAI-HOON KIM[3], (Member, IEEE)

[1]School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India
[2]School of Electronics and Communication Engineering, Lovely Professional University, Phagwara 144411, India
[3]Department of Convergence Security, Sungshin Women's University, Seoul 02844, South Korea

Corresponding author: Rahul Saha (rsahaaot@gmail.com)

ABSTRACT Vehicular ad hoc networks (VANETs) have been considered as one of the most influential applications of mobile ad hoc networks. The VANETs have also become an important part of Internet of Things. Along with the advantages, such networks are facing a number of security issues. A number of research have been done so far to identify the solution of the security problems in the VANETs. But the existing solutions do not confirm the confidentiality-integrity-availability (CIA) triad services simultaneously. Therefore, in this paper, we have provided a solution for the VANETs security using end-to-end authentication to avoid intrusion in the VANETs. After verifying the communicating entities, the data are transmitted in encrypted form thus the proposed approach provides CIA security services to VANETs communication. Along with this, we have used a sandboxing method for in-vehicle communication for prevention of intrusion in form of downloaded information. Moreover, in this paper, the VANETs are considered as a hierarchical model to concentrate on a less number of message exchanges. Furthermore, the simulation results show the efficiency of our proposed solution.

INDEX TERMS Authentication, certificate, hierarchical, multidimensional, security, VANETs.

I. INTRODUCTION

The exponential growth of the socio-economic life of human beings and their increasing demand for enhancing the lifestyle lead to the rapid line up of private vehicles on roads. Fast and furious life with such vehicles is also alarming to the death tolls and other hazards. The increasing traffic on roads has always been crucial point of consideration in every country. Therefore, to manage such traffic and also to avoid the problems on roads, Mobile Ad hoc Networks (MANETs) has been extended to an application of vehicles, called as Vehicular Ad hoc Networks (VANETs) [1]. In such networks, the vehicles use the dedicated short range communication with other vehicles or to the road-side infrastructure in ad hoc manner. Communication in a VANETs allows vehicles to share different kinds of information such as safety information for the purpose of accident prevention, post-accident analysis or traffic congestion. Moreover, non-safety information such as car related information can also be gathered for detecting criminal activities.

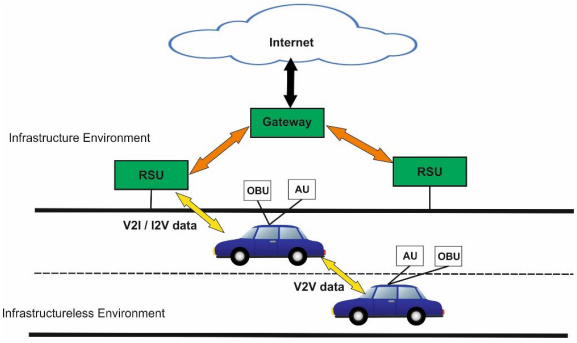

FIGURE 1. Basic architecture of VANETs.

The basic architecture of VANETs [2], [3] is shown in Figure 1. The architecture for such network is comprised of two types of network: the infrastructureless part deals with the ad hoc vehicles and the infrastructure oriented part deals with Road Side Units (RSUs) basically. Each vehicle is equipped

with an On Board Unit (OBU) and a set of sensors to collect and process the information in form of messages. These messages are sent to other vehicles or RSUs as required for the purpose of Vehicular-to-Vehicular (V2V) or Vehicular-to-Infrastructure (V2I) communication respectively. The vehicles are also equipped with a single or multiple Application Unit (AU). AUs use the applications provided by the provider using OBU connection capabilities. On the other hand, RSUs are placed at traffic signals, parking areas or even at specific locations on the sides of roads. These RSUs have two types of network devices: one used for dedicated short range radio transmission and another is used to communicate in between infrastructure components. The RSU can also connect to the Internet or to another server which allows AU's from multiple vehicles to connect to the Internet.

The VANETs communications can be logically categorized in three domains as shown in Figure 2. The categories include in vehicle domain, ad hoc domain and infrastructure domain [4]. The in vehicle domain of communication deals with the interfacing between OBUs and AUs, ad hoc domain communication is done among the vehicles or between a vehicle and RSUs. Infrastructure domain communication is processed by RSUs, gateways and Internet components. The VANETs deal with the traffic information primarily. Though the sensitive or confidential information is not shared with such network such as Wireless Sensor Networks, but several attacks exploits the vulnerabilities of VANETs which leads to the misleading traffic information, false route navigation or even denial of services to exhaust the resources or the VANETs. Table 1 summarizes the attacks in different types of domain of communication in VANETs [31], [32].

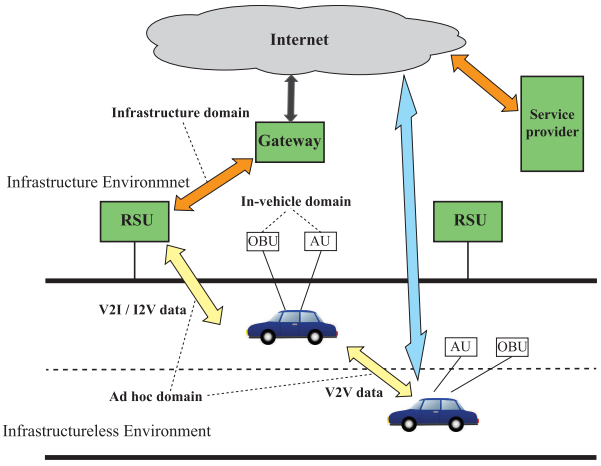

FIGURE 2. Categories of communication domains in VANETs.

Attacks in In-Vehicle Domain: These attacks attempt to get access of the OBUs or AUs by spoofing valid IDs through RSUs. A severe attack may also indulge with exploiting a malicious code to the AUs which may lead to the malfunctioning of the devices. As VANETs applications include active road safety, infotainment, traffic efficiency and management, chances of such attacks are larger [5].

TABLE 1. Summarization of Attacks.

In-vehicle domain	Remote Accessing, Shellcoding
Ad hoc domain	Authentication attacks, replay attacks, routing attacks
Infrastructure domain	Routing attacks, DDoS attacks

Attacks in Ad Hoc Domain: These attacks spoof the legitimate IDs and intercepts the VANETs communication. Some attackers also capture the packets and replay it with falsified information.

Attacks in Infrastructure Domain: The prime objective of attackers in this domain of communication is to exhaust the VANETs resources by sending a number of messages to a particular RSU or a number of RSUs at a time in a part of the city. Misleading localization is also another part in these attacks.

Apart from the above attacks, co-channel existence and interference of signals are also crucial in VANET environment. These techniques are used by the eavesdroppers to execute passive attacks. Several methods including successive interference cancellation [6], on demand interference aware routing algorithm [7], media access control protocol and cluster [8], secure multiple amplify and forward relaying [9], outdated relay selection process [10] can be used to prevent these attacks.

In VANETs, it is very crucial to provide the safety guard against misuse activities or malicious exploitation. The predefined security requirements and its guaranteed level of implementation affect people safety. Many researchers have explored the security attacks in VANETs and have proposed related solutions. Moreover, secure infrastructures, or formalized standards and protocols are also have been introduced. But, the trend of trustworthiness of a node in VANETs communication and misbehaving detection is large to explore. In this paper, therefore, we have proposed a scheme to provide the basic security services in hierarchical trust management to provide a secure VANETs infrastructure. The main contributions of this paper are summarized as follows:

- The proposed approach emphasizes to provide CIA security services in VANETs architecture.
- The proposed approach follows a hierarchical model to utilize the minimum number of message exchange.
- We have used elliptic curve cryptography for confidentiality and end-to-end authentication for integrity and availability.
- The proposed approach uses sandboxing method for in-vehicle security of downloaded services.

The rest of the paper is organised as follows. Section 2 reviews the existing research work in the same direction. Section 3 proposes our algorithm. Section 4 shows the related results and discussions and finally Section 5 concludes the paper.

II. RELATED WORK

The present technology is converging to the IoTs ventures and combining it with information and communication technology. VANETs are one of the important part of this. A number of research has been executed in this domain. Some of the recent works are mentioned below.

A new data retrieval scheme has been proposed in [11] providing the robustness of the backbone. The proposal withstands for denial of service attacks and also decreases the length of nodes' request messages. The proposed algorithm is adaptive for both symmetric and asymmetric cryptographic algorithms. The complexity of the key signatures is a drawback in this algorithm. A group-key based protocol for VANETs has been introduced in [12]. The algorithm uses a password based conditional privacy preserving approach. Though the algorithm provides solutions for security issues but computational complexity with create the delay in transmission. Another conditional privacy preserving approach has been shown in [13]. The proposed approach uses an identity based scheme that consists of the system initialization phase, the anonymous identity generation and message signing phase and the message verification phase. An authentication scheme has been proposed for the VANETs architecture in [14].The authentication scheme depends on a key agreement protocol. The proposed approach contains of four phases: system setup phase, user registration phase, user login and authentication phase, password change phase. The cost of the algorithm is significantly less but the packet delay ratio has a drawback factor. A secure multimedia message delivery scheme has been proposed in [15]. It uses AES for confidentiality and SHA-256 for hashing. Though the process provides strong encryption and end device verification, it does not provide end to end authentication process which may lead to authentication attacks. A key based approach has been described in [16]. The authors have used multiple session keys but have not provided solution for session hijacking attacks. A secure message delivery approach for VANETs has been suggested in [17]. The proposed approach uses group key and symmetric key for the authentication of messages. The use of group key must be secure which has not been significantly shown. Utilization of cryptographic algorithms has also been shown in [18], where the authors have used attribute encryption techniques. The access policies are also considered for the proposed approach. Confidentiality of the message dissemination has been maintained in this algorithm but the authentication message, integrity and non-repudiation have not been ensured.

Apart from the key-based approaches, some trust based approaches are also researched in recent time for secure communication in VANETs. Such a trust based approach is seen in the work [19]. The proposed approach provides reliability and accuracy of the messages but does not provide and man-in-the-middle attack prevention provision. A game theory based trust model for VANETs has been shown in [20]. The proposed model works on an attacker and defender security game to identify and counter the malicious nodes. Majority opinion, betweenness centrality and node density are considered as parameters for the model. The use of Nash equilibrium model and priority of the defender nodes do not ensure the DoS attacks. The falsified trust or the insider malicious nodes are another problem for this approach. A trust based framework for reliability is observed in [21]. The proposed algorithm confirms reliability issue but does not provide authentication solutions. A dynamic entity centric approach for trust oriented framework has been developed in [22]. Though he trust factor is determined significantly in the proposed approach, but the application privacy is not claimed.

Analysing the previous work in VANETs for security provisions, we have identified the major problems with the existing algorithms that they are not ensuring the overall security services for VANETs. The cryptographic approaches are well defined but they lack in their complexities and unnecessary overhead. Whereas, the trust based approaches provide only reliability of the communication and but have not significantly addressed the issue of secure communication. Moreover, the message transmission concentration depends upon the traffic density in a particular point, that's why we need to develop a hierarchical structure where the OBUs are used less as they are battery powered. Therefore, in this paper, we have proposed an approach that provides multidimensional security in VANETs using a hierarchical architecture.

III. PROPOSED SYSTEM MODEL

We have introduced the hierarchical architecture of VANETs. This architecture is comprised of RSU Controller, Zone Controller and Certificate Authority to provide maximum security in the infrastructure domain communication. RSU Controller controls a number of RSUs (for example: road 1 and road 2), Zone Controller controls the communication in a particular area which may have multiple RSU controllers. The proposed architecture is shown in Figure 3. The infrastructure environments of VANETs are proposed to have a single Certification Authority (CA). The CA distributes the certificates to all the components of infrastructure.

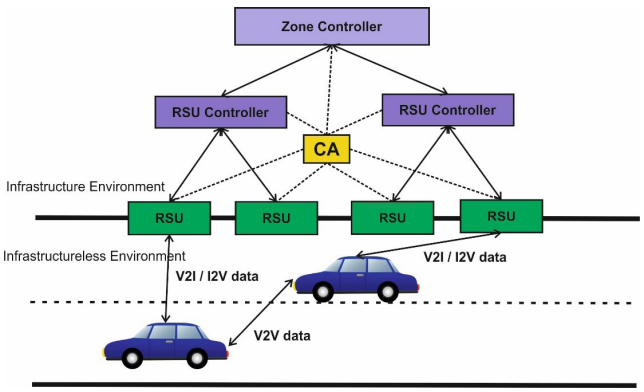

FIGURE 3. The proposed hierarchical architecture of VANETs.

We have also considered some assumptions as follows.

- CA is responsible for the certificate and key distribution.
- The VANETs provide a fixed set of services or applications
- The cryptographic keys are controlled by CA itself i.e. CA distributes its corresponding public keys to all he units predefined.
- The elements of the infrastructure environment communicates with the one-hop neighbours only. For example, if a message of road accident is need to be distributed, RSUs send the message to one hop RSU Controllers, RSU Controller send it to Zone Controller and finally Zone Controller distributes the message accordingly.
- Keys update done with predetermined expiration schedule.
- RSU uses a variable threshold value of message control in a particular time interval which depends on the traffic congestion.

The abstraction map M for the above network architecture has been considered as a rectangle. It provides a mathematical model for understanding the system model for our experiment. The communication range of RSUs and vehicles is r. We have partitioned the map M in some squares having $1m^2$ area. The RSU at the centre of the grid square with this length and height is accessible from a VANETs node in any location within the grid square. The concept is shown in the figure 4.

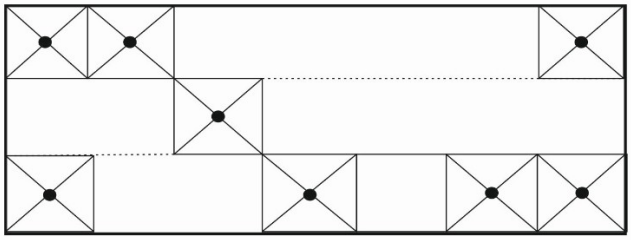

FIGURE 4. Abstraction of the network map in the system model.

IV. PROPOSED ALGORITHM

Security in VANETs, as discussed in earlier sections, is an important issue. To overcome the drawbacks of the existing solutions as discussed in section 2, we have defined some objectives for our proposed solution for the security issues. The objectives are shown in Table 2.

The proposed solution for the security issues in VANETs is categorized in two segments: security in in-vehicle communication and security in ad hoc or infrastructure domain.

A. SECURITY OF IN-VEHICLE COMMUNICATION

The security exploitation in in-vehicle communication can be done by the remote accessing methods or even by using the internet services from the road side RSUs. Therefore, before accessing the services the vehicle requesting for the service or application, must be verifying the service provider by certificate verification. The process starts by the OBU of a vehicle that sends the required service id ($service_{id}$), vehicle id (v_{id}) and certificate of the vehicle ($cert_v$) to the service provider or to the RSU. The certificate is then verified from the certificate authority. After the verification, the service or the application is granted. The OBU also needs to verify the certificate of the service provider ($cert_p$) and after the verification it starts using the service or application in AU. Once the use of the application is over, the OBU sends finish message (FIN=1) to the service provider. The process is summarized as shown in Figure 5. To get the further protection from shell codes, the AU must be installed with sandboxing feature. Sandboxing is an alternative to traditional signature based malware defense techniques. This is to be used in the vehicles as a process to detect shell code patterns, Zero-day vulnerability and stealthy attacks in VANETs communication [33], [34].

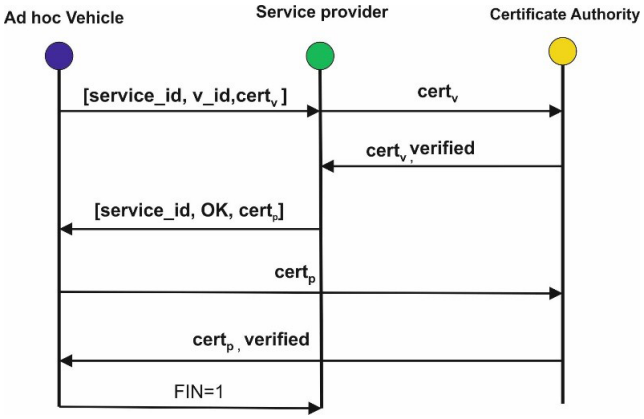

FIGURE 5. Proposed interaction among entities for in-vehicle secure communication.

TABLE 2. Objectives of proposed solution.

Message Integrity	The objective is to check that the the message cannot be altered or tampered in between of messages transmission.
Source authentication	The source of messages should be efficiently authenticated attack to prevent impersonation.
Low storage space usage	As OBUs have limited storage space, the minimum usage need to be executed on them for any of the process.
Low communication overhead	The authentication or confidentiality process should not create communication overhead in the transmission media or on the participating entities.
Fast verification and efficient dissemination	Messages need to be verified and disseminated quickly and efficiently to all relevant users in regions covered by various RSUs.

B. SECURITY IN AD HOC AND INFRASTRUCTURE COMMUNICATION

Security applications in ad hoc domain communication and infrastructure domain communication emphasize two dominant facts: the proposed hierarchical architecture of VANETs and end-to-end authentication process using certificates from CA.

1) KEYS AND CERTIFICATE ESTABLISHMENT

CA provides the identity for all RSUs, RSU Controllers and Zone Controllers as ID_{RSU}, ID_{RSU_C} and ID_Z respectively. It also provides certificates for each elements denoted previously as $Cert_RSU$, $Cert_{RSU\_C}$ and $Cert_Z$.

$$CA \rightarrow Cert_{RSU} = [ID_{RSU}, K_{RSU+}, e]CA_{K-} \quad (1)$$

$$CA \rightarrow Cert_{RSU\_C} = [ID_{RSU\_C}, K_{RSU_{C+}}, e]CA_{K-} \quad (2)$$

$$CA \rightarrow Cert_Z = [ID_Z, K_{Z+}, e]CA_{K-} \quad (3)$$

Where, $K_{RSU+}$is the public key of RSU, $K_{RSU_{C+}}$ is the public key of RSU Controller, K_{Z+} is the public key of Zone Controller and e is the expiry time of the certificate. This total certificate is digitally signed by CA_{K-} which is the private key of the Certificate Authority (CA). All the entities of the infrastructure must make them updated itself by having a fresh certificate as required.

2) MESSAGE FROM VEHICLE TO RSU

A vehicle willing to send message generates a request message RQST with its v_{id} and expiry timestamp t_{exp} and broadcasts it. The receiving RSU checks the threshold value $m_{threshold}$ of message control and also checks t_{exp}. If the incoming messages are less than the threshold and t_{exp} is not expired, it replies back with an acknowledgment of receiving response message RSPN. If the incoming messages are greater than the threshold value, the RSU sends an alarm notification flag turned on i.e. ALRM = 1. Receiving this message, Deffie-Hellman key exchange [23] is executed between RSU and the vehicle. Once, the vehicle receives the keys, it sends the message M by encrypting the message with Elliptic Curve Cryptography (ECC) [30] and generating a digest of the message H(M). This message digest helps the RSU in verifying the authenticity and the integrity of the messages. Note that the RSU to which the message is sent may not be within the transmission range of the vehicle sending a message and hence a secure routing protocol [24] is used for routing the messages. The process is summarized in Algorithm 1. The complexity of Algorithm 1 is $O(N)$ where N is the number of vehicles communicating to a particular RSU.

3) MESSAGE FROM RSU TO INFRASTRUCTURE COMPONENTS

Once a RSU is receiving message from the vehicle, it is forwarded to the RSU controller along with its own certificate and validity time duration t_v. If time validated, RSU controller acknowledges RSU with a response and also sends the message to Zone controller with required certificate.

Algorithm 1 Message Processing From Vehicle to RSU

1: Vehicle broadcasts: $RQST$ $\{v_{id}, t_{exp}\}$
2: **if** *message_count* $<$ $m_{threshold}$ *and* t_{exp} *is not expired* **then**
3: $RSU \rightarrow vehicle$: $RSPN\{ID_{RSU}, t_s\}$ ▷ where t_s is the timestamp of the message sent
4: **else**
5: RSU broadcasts: ALRM=1
6: **end if**
7: Vehicle → RSU: Deffie-Hellman key Exchange
8: Vehicle → RSU: ECC on message M, H(M)
9: Executing Secure Routing Protocol

If timestamp is expired, RSU controller broadcasts a notification message NOTIFY with T_INVALID flag turned on. End-to-end authentication is applied to securely transfer the message to Zone controller for further processing. The steps are given in Algorithm 2. In this algorithm each transaction of certificates takes the time in $O(N)$ where N is the number of vehicles. If t_v is valid total three transactions are processed. So, the time complexity becomes $O(3N) \equiv O(N)$. Similarly if t_v is invalid two transactions are processed and time complexity becomes $O(2N) \equiv O(N)$.

Algorithm 2 Message Processing From RSU to Infrastructure Components

1: $RSU \rightarrow RSU\ Controller$: $\{[M]_{RSU_{K-}}, Cert_{RSU}, t_v\}$
2: **if** t_v *is valid* **then**
3: $RSUController \rightarrow RSU : ACK_{RSU_C}\ Cert_{RSU\_C}$
4: $RSUController \rightarrow ZoneController$: $\left[[M]_{RSU_{K-}}\right]_{RSU\_C_{K-}}, Cert_{RSU\_C}$
5: **else**
6: $RSU\ Controller\ broadcasts$: $NOTIFY$ {T_INVALID= 1}
7: **end if**
8: Zone controller saves the message for further processing by decrypting the message and getting original M

4) INFORMATION DISTRIBUTION FROM ZONE CONTROLLER

Once the Zone controller receives the messages, it checks the time stamp of receiving the message t_r and sends the message to base stations and other zone controllers so that every zone controller is updated with required information.

5) VEHICLE MOBILITY HANDLING

The vehicles are considered to be moving with an average velocity v, which can be detected from the in-vehicle OBU. So, whenever a vehicle is sending a query or message through RSU, RSU Controller upto Zone controller, it is obvious that the same Zone controller or RSU controller will to be responsible for the responses to the vehicles. Every zone controller is having an average operation radius $\mathcal{R}$. The propagation time of the message ($time_{prop}$) from vehicle (v_{id}) to the zone

controller z_i is calculated as:

$$time_{prop} = t_r - t_s \tag{4}$$

Therefore, the probable distance the vehicle (v_{id}) moves a distance of :

$$dist = time_{prop} \times v \tag{5}$$

If the dist $> \mathcal{R}$, then zone controller z_i sends the message to its neighbour zone controller z_{i-1} or z_{i+1} depending upon the direction of the vehicle following the end-to-end authentication [25] so that the responses can be given to the required vehicle.

The query and response mechanism is very frequent in the events of VANETs and therefore the availability of the responses must be insured in less time. To enhance the availability and add-on the reliability of the data transmission cache aided design is used with decode-and-forward relaying method as depicted in [26]. This cache aided design also helps to perform better in processing in an environment even with outdated channel state information [27]. In our proposed approach cache aided design is implemented with the RSUs with 5Gb R1 cache memory this design has significantly reduced the processing time for the query generated by the multiple vehicles.

C. HANDLING AVAILABILITY

Availability in security emphasises that the data must be available at request to the legitimate party. Distributed Denial of Service (DDoS) attacks, void routings are major challenges for such availability issues. The use of End-to-End Authentication with certificates reduces the probability of DDoS attacks launched by any intruder. Moreover, sandboxing in individual vehicle eliminates the problem of being a slave in remote DDoS attacks. The use of time stamp handles the issue of void routing. Furthermore the cache aided design also helps for the purpose.

V. RESULTS AND ANALYSIS

We have used the VANETs simulation environment from the ezCar2X framework. Along with this environment SUMO [28] is used to provide realistic traffic flow simulation, and ns-2 is used to simulate both physical and access layer. Further ETSI ITS specific functionality is provided by the full protocol stack implementation from ezCar2X. A highway scenario with two lanes in up and down direction and a length of five kilometers is used during our evaluation. The traffic density is varied between only a single vehicle on the road up to a maximum average vehicle interval on both the lanes of ten seconds. SUMO's random traffic flow generator is used for obtaining the traffic flow. The simulation terminates after 1000 vehicles have passed through the whole simulated highway section. A node tries to obtain a new certificate with an interval of 5 s following the proposal in [29]. The Certificate Authority (CA) used in the simulation environment is assumed to be able to process a single request from every valid node within one second. This means, if all nodes would sent their request within an interval of one second assuming highest regarded traffic density, the CA is able to process all requests. Dropping of requests is also executed following the threshold value in the algorithm. Successful and failed signature verifications are assumed to take equal processing time.

The proposed model is compared with three recent algorithms in this domain of work: [11], [14], and [15]. The comparison of the results has been done in three categories: cost analysis, security performance and network performance.

A. COST ANALYSIS

The cost analysis of the algorithms has been executed in two ways: computation cost and communication cost.

In any authentication protocol the computation cost determines the total cost of protocol, which should be as minimum as possible. Table 3 shows the computational cost of the algorithms. Vehicles, RSUs, RSU controllers and Zone controllers are involved in the overall process of message dissemination including authentication and encryption. We calculate the computation cost by considering T_v, T_p and T_x as time of a certificate verification operation ($\approx$ 0.0025 sec.), time of a cryptography operation ($\approx$ 0.0080 sec.), time of a cryptographic message exchange ($\approx$ 0.0030 sec.) respectively. The results show that, our protocol has lesser

TABLE 3. Computation cost comparison.

Schemes	Vehicle	RSU	RSU controller	Zone controller	Total cost	Total cost (sec)
Mohit et. al. [14]	$4T_v + 4T_p + 3T_x$	$3T_v + 4T_p + 2T_x$	$2T_v + 3T_p + 2T_x$r	NA	$9T_v + 11T_p + 7T_x$	0.1315
Bittl et. al. [11]	$8T_v + 7T_p + 4T_x$	$6T_v + 6T_p + 4T_x$	$3T_v + 4T_p + 4T_x$	NA	$17T_v + 17T_p + 12T_x$	0.2145
Karanki et al. [15]	$5T_v + 10T_p + 9T_x$	$5T_v + 10T_p + 8T_x$	$5T_v + 7T_p + 7T_x$	NA	$15T_v + 27T_p + 24T_x$	0.3255
Proposed algorithm	$2T_v + 2T_p + T_x$	$1T_v + 2T_p + 3T_x$	$1T_v + 2T_p + 3T_x$	$1T_v + 2T_p + 3T_x$	$5T_v + 6T_p + 10T_x$	0.0905

computation overhead, then all the compared algorithms and therefore is suitable for practical application.

Table 4 shows the communication cost of our proposed approach with the related algorithms. The communication cost is measured in terms of bits length. The algorithm depicted in [14], 160 bits SHA-1 hash function is used along with timestamp, identity, random number, nonce are of 64 bits each. Moreover user identity is 160 bits and user temporary identity is 160 bits. ECC- point multiplication is used with 512 bits and symmetric key encryption/decryption is 256 bits. Thus, communication cost of this protocol is 1280 bits as computed between user, sensor and sink node. The algorithm depicted in [11] uses a 66 byte certificate i.e 528 bits and uses SHA-512 having 512 bits digest to be used. These two processes itself taking >1000 bits and therefore, considering time stamps and identities and other attributes of 64 bits each, the communication cost is greater than the previous algorithm. The algorithm used in [15] uses SHA-256 producing 256 bits digest. Assuming key size of 256 bits, AES of 256 bits and random number of 64 bits and some other processes, the algorithm in [15] uses approximately 1000 bits. Lastly, our proposed algorithm uses certificate of 64 bytes i.e. 512 bits with Deffie-Hellman key exchange of 160 bits, time stamp of 64 bits, identities of 64 bits each and asymmetric encryption of 128 bits; therefore, overall 928 bits are used for communication.

TABLE 4. Simulation parameters and rules.

Schemes	Communication cost (bits)
Mohit et. al. [14]	1280
Bittl et. al. [11]	>1280
Karanki et al. [15]	≈ 1000
Proposed algorithm	928

B. SECURITY PERFORMANCE

The major problems of VANETs shown in Table 1 have been solved by our proposed algorithm as in Table 5.

TABLE 5. Solution for VANETs problems.

	Type of Attacks	Solution provided in the proposed algorithm
In-vehicle domain	Remote Accessing Shell coding	Validation of certification Sandboxing applications in OBU
Ad hoc domain	Authentication attacks Replay attacks Routing attacks	End-to-end authentication process Time validation Secure routing protocol Use of cache
Infrastructure domain	Routing attacks DDoS attacks	Secure routing protocol Threshold value of message count

The above table depicts that our proposed approach for security provision is able to prevent security attacks in different layers of VANETs' architecture. We have further computed the time consumption by the security procedures for a message with different environment of speed and car density as shown in Table 6. The average speed of the cars is categorized into: 25 km/ hour, 60 km/hour and 90 km /hour. Car density is calculated as number of cars running through a particular square area in unit time.

Furthermore, we have also compared our results with existing algorithms in terms of processing efficiency which has been measured as processing time vs. message size. The results in Figure 6 show that processing time in our proposed approach is less with short messages. Processing time increases with increasing message size. regards of processing efficiency with increasing message length.

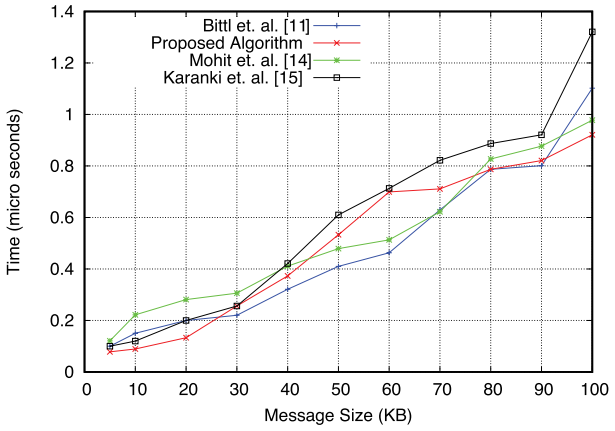

FIGURE 6. Comparison of processing time vs. Variable message size.

We have introduced a parameter called "Validity Ratio" (V_R) defined as the ratio between the total number of valid messages and total number of invalid messages traversing in the VANETs scenario and as given by:

$$V_R = \frac{R_I}{R_V} \tag{6}$$

where, R_I is number of invalid requests and R_V is the number of valid requests. The above parameter is also compared with the other algorithms in comparison. The result of the comparison in Figure 7 shows an efficient attribute of our proposed

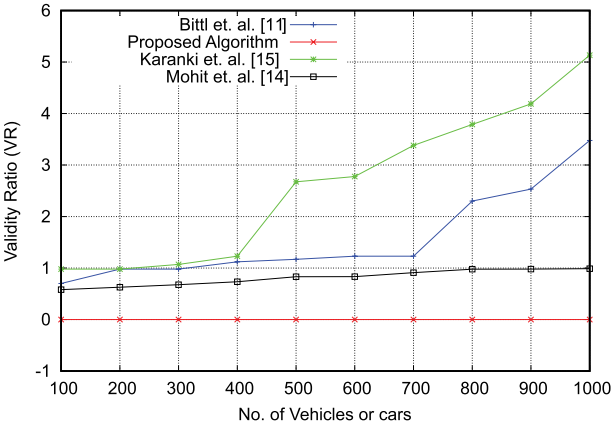

FIGURE 7. Comparison of validity ratio vs. No. of Vehicles.

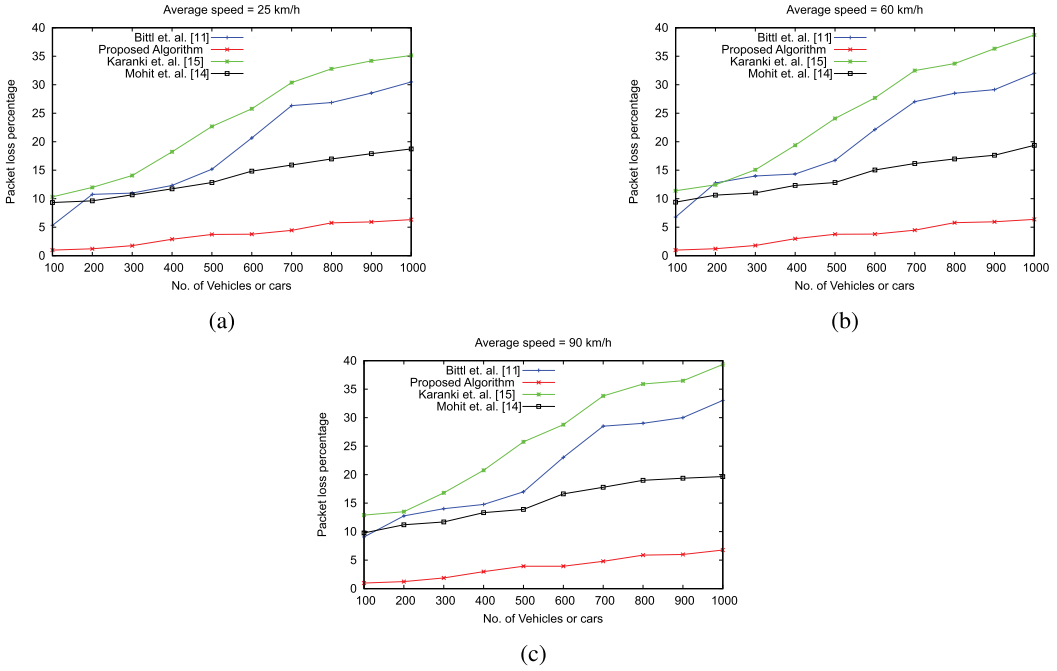

FIGURE 8. Comparison of packet loss percentage vs. No. of vehicles.

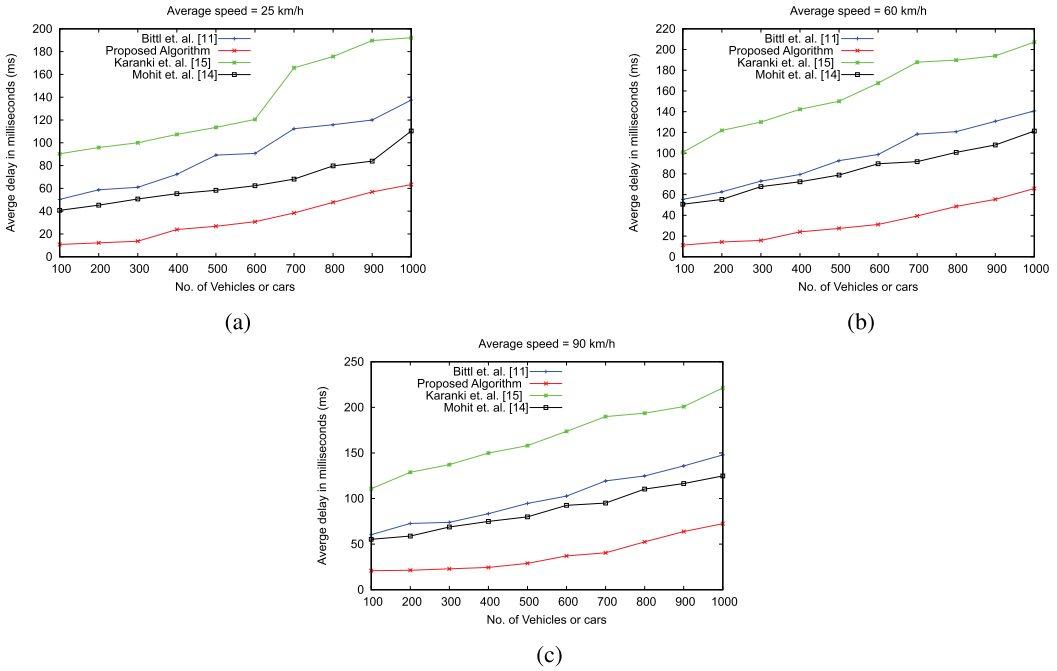

FIGURE 9. Comparison of average delay vs. No. of vehicles.

algorithm that even though there are increasing number of cars in the environment, invalid messages are prohibited in the network and therefore in the Figure 7 it follows a straight line at value 0.

C. NETWORK PERFORMANCE

We have evaluated the performance of the proposed VANETs architecture in the terms of packet loss percentage and average delay. The results are also compared with the existing algorithms of Brittl [11], Mohit *et al.* [14], and Karanki and Khan [15].We have considered three average speed scenarios as: 25km/hr, 60 km/hr and 90 km/hr. The results are shown in the Figure 8 by varying the number of cars and simulating the environment for evaluation of packet loss percentages. The results show that in all the speed scenarios, our proposed algorithm outperforms the other algorithms and is not

TABLE 6. Time analysis and comparison of cryptographic procedures of the algorithms.

Hardware specification for computation: CPU: 2.6Ghz, i3 6th,Gen with 16 GB RAM							
		Average Speed			Car Density		
Schemes	Message size	25 km/h	60 km/h	90 km/h	<10 cars	11-20 cars	>20 cars
Mohit et. al. [14]	1000 bytes	5.67	5.73	5.92	8.98	9.17	9.89
Bittl et. al. [11]	1000 bytes	5.78	5.87	5.99	10.78	11.20	12.52
Karanki et al. [15]	1000 bytes	6.55	6.73	6.93	19.76	20.13	20.87
Proposed algorithm	1000 bytes	4.63	5.12	5.33	6.72	7.23	7.55
Values are given in microseconds							

affected by the increased average speed of the cars. We have also found that the packet loss percentages gets saturated at the maximum value as shown in Figure 8 when number of vehicles are taken more than 1000.

Delay in transmission of messages is an important QoS in network performance evaluation. We have evaluated this parameter by comparing with other existing algorithms as above. We have calculated the average delay in accordance with increasing number of cars. Three different average speed scenarios have been considered as previous. The results are shown in Figure 9. The results depict that our proposed algorithm is better than the other algorithms in comparison in terms of transmission delay. We have measured the efficiency of the proposed approach with cache aided design in comparison with other existing algorithms. The result shown in Figure 10 depicts that the processing time for resolving the same query from multiple vehicles is reduced significantly. We can also find from the figure that the other existing algorithms in comparison are having increased processing time as they are not using he cache memory.

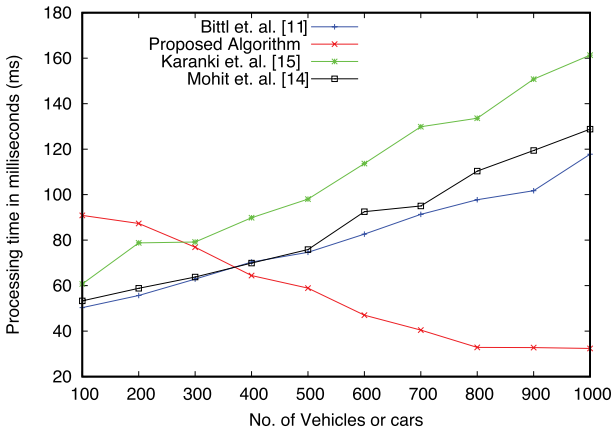

FIGURE 10. Comparison of processing time based on cache.

VI. CONCLUSION

VANETs are the important part in our present technology progress of IoTs. A number of solutions have been provided by previous works but they do not conceptualize the traffic overhead due to excessive use of cryptographic parameters exchange. In the proposed approach, we have used a hierarchical architecture of message transmission using elliptic curve cryptography and end-to-end authentication to provide message integrity and authentication. We have also used sandboxing method for in-vehicle security. We have compared the simulated results of our approach with some existing protocols with respect to cost, security and network performance. The results show that our proposed algorithm is better than the other algorithms in providing security and incurring less cost. Though the processing time increase with the increasing number of message size. In our future work, we shall work upon the optimization of hierarchical structure for minimum message transmission and faster processing.

ACKNOWLEDGMENT

G. Kumar, R. Saha, and M. K. Rai conceived the idea, designed the experiments, and analyzed the data; G. Kumar and R. Saha performed the experiments and conducted the analyses; T. Kim interpreted the results and drew the conclusions; and R. Saha wrote the paper. All the authors declare no conflict of interest.

REFERENCES

[1] P. M. Khilar and S. K. Bhoi, "Vehicular communication: A survey," *IET Netw.*, vol. 3, no. 3, pp. 204–217, 2014.
[2] J. A. C. Guerrero–Ibáñez, C. Flores-Cortés, and S. Zeadally, "Vehicular ad-hoc networks (VANETs): Architecture, protocols and applications," in *Next-Generation Wireless Technologies*. London, U.K.: Springer, 2013, pp. 49–70.
[3] W. Liang, Z. Li, H. Zhang, Y. Sun, and R. Bie, "Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 8, pp. 102–113, 2015.
[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.
[5] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.
[6] S. Sen, N. Santhapuri, R. R. Choudhury, and S. Nelakuditi, "Successive interference cancellation: A back-of-the-envelope perspective," in *Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw. (Hotnets-IX)*, 2010, Art. no. 17.
[7] P. Fazio, F. De Rango, and C. Sottile, "A new interference aware on demand routing protocol for vehicular networks," in *Proc. Int. Symp. Perform. Eval. Comput. Telecommun. Syst.*, The Hague, The Netherlands, 2011, pp. 98–103.
[8] K. A. Hafeez, L. Zhao, J. W. Mark, X. Shen, and Z. Niu, "Distributed multichannel and mobility-aware cluster-based MAC protocol for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 3886–3902, Oct. 2013.
[9] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.
[10] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug. 2017.

[11] S. Bittl, "Privacy conserving low volume information retrieval from backbone services in VANETs," *Veh. Commun.,* vol. 9, pp. 1–7, Jul. 2017.
[12] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2017.
[13] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[14] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Veh. Commun.*, vol. 9, pp. 64–71, Jul. 2017.
[15] S. S. Karanki and M. S. Khan, "SMMV: Secure multimedia delivery in vehicles using roadside infrastructure," *Veh. Commun.*, vol. 7, pp. 40–50, Jan. 2016, doi: 10.1016/j.vehcom.2016.12.002.
[16] C.-C. Lee, Y.-M. Lai, and P.-J. Cheng, "An efficient multiple session key establishment scheme for VANET group integration," in *Proc. IEEE Intell. Syst.*, vol. 31, Jun./Jul. 2016, pp. 35–43.
[17] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Veh. Commun.*, vol. 4, pp. 30–37, Apr. 2016.
[18] X. Liu, Y. Xia, W. Chen, Y. Xiang, M. M. Hassan, and A. Alelaiwi, "SEMD: Secure and efficient message dissemination with policy enforcement in VANET," *J. Comput. Syst. Sci.*, vol. 82, no. 8, pp. 1316–1328, Dec. 2016.
[19] S. Goli-Bidgoli and N. Movahhedinia, "Determining vehicles' radio transmission range for increasing cognitive radio VANET (CR-VANET) reliability using a trust management system," *Comput. Netw.*, vol. 127, pp. 340–351, Nov. 2017, doi: 10.1016/j.comnet.2017.07.017.
[20] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for vehicular ad hoc networks (VANETs)," *Comput. Netw.*, vol. 121, pp. 152–172, Jul. 2017.
[21] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," *Veh. Commun.*, vol. 9, pp. 254–267, Jul. 2016, doi: 10.1016/j.vehcom.2016.11.010.
[22] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.
[23] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[24] M. Altayeb and I. Mahgoub, "A survey of vehicular ad hoc networks routing protocols," *Int. J. Innov. Appl. Stud.*, vol. 3, no. 3, pp. 829–846, 2013.
[25] G. Kumar, R. Saha, and M. K. Rai, "Improvement of trust and reputation using intrusion detection and authentication in ad hoc networks," *Int. J. Secur. Appl.*, vol. 10, no. 4, pp. 63–70, 2016.
[26] J. Xia *et al.*, "Cache aided decode-and-forward relaying networks: From the spatial view," *Wireless Commun. Mobile Comput.*, vol. 2018, Apr. 2018, Art. no. 5963584.
[27] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 21879–21887, 2018.
[28] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO—Simulation of urban MObility: An overview," in *Proc. 3rd Int. Conf. Adv. Syst. Simulation*, 2011, pp. 63–68.
[29] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in VANETs," in *Security and Privacy in Ad-Hoc and Sensor Networks* (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Berlin, Germany: Springer, 2006, pp. 43–57.
[30] A. H. Koblitz, N. Koblitz, and A. Menezes, "Elliptic curve cryptography: The serpentine course of a paradigm shift," *J. Number Theory*, vol. 131, pp. 781–814, May 2011.
[31] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[32] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.
[33] N. Nikaein, S. K. Datta, I. Marecar, and C. Bonnet, "Application distribution model and related security attacks in VANET," *Proc. SPIE*, vol. 8768, p. 876808, Mar. 2012.
[34] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: Paradigms, scenarios, and issues," *J. China Universities Posts Telecommun.*, vol. 23, no. 2, pp. 56–66, 2016.

GULSHAN KUMAR received the B.Tech. degree in computer science engineering from the Amritsar College of Engineering and Technology, Amritsar, in 2009, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Phagwara, India, with a focus on position and location computation in wireless sensor networks. He is currently an Assistant Professor with Lovely Professional University. He has many publications in well renowned international journals and conferences.

RAHUL SAHA received the B.Tech. degree in computer science engineering from the Academy of Technology, West Bengal, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Phagwara, India, with a focus on cryptography, and position and location computation in wireless sensor networks. He is currently an Assistant Professor with Lovely Professional University. He has many publications in well renowned international journals and conferences.

MRITUNJAY KUMAR RAI received the M.E. degree in digital system from the Motilal Nehru National Institute of Technology, Allahabad, India, and the Ph.D. degree from the ABV Indian Institute of Information Technology and Management, Gwalior, India. He is currently an Associate Professor with Lovely Professional University, Phagwara, India. He has published over 50 research articles in reputed international conferences and international journals. His research interests include wireless networks, network security, and cognitive radio networks.

TAI-HOON KIM received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degrees from the University of Bristol, U.K., and the University of Tasmania, Australia. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.