Insight to Research Progress on Secure Routing in Wireless Ad hoc Network

Jyoti Neeli
Dept of Information Science & Engineering
Global Academy of Technology
Bengaluru,
India

N K Cauvery
Professor & HOD
Dept. of Information Science of Engineering
RV College of Engineering,
Bengaluru, India

***Abstract*—Wireless Ad hoc Network offers a cost effective communication to the users free from any infrastructural dependencies. It is characterized by decentralized architecture, mobile nodes, dynamic topology, etc. that makes the network formation typically challenging. In the past decade, there has been a series of research work towards enhancing its routing performance by addressing various significant problems. This manuscript mainly orients around the progress being made in the line of secure routing protocol, which is still a bigger issue. The paper discusses different approaches undertaken by existing literature towards discrete security problem and explores the effective level of security. The study outcome of the paper finds that progress towards wireless ad hoc network is still very less and there is a need to come up with robust security framework. The paper also discusses the research gap being identified from the existing techniques and finally discusses the future work direction to address the certain unsolved problem.**

***Keywords*—Attacks; confidentiality; secured routing; integrity; mobile ad hoc network; wireless ad hoc network**

I. INTRODUCTION

Wireless ad hoc network consists of autonomous nodes that are interconnected by themselves without any presence of infrastructure [1]. It is highly useful for offering robustness communication with minimal cost. The sustenance of wireless ad hoc network is quite high irrespective of any adverse deployment area [2]. For this reason, there is wide range of applications using ad hoc network e.g. recovery from natural disaster, combat, and military application, community network, etc. However, there are multiple challenges in the design principle of the wireless ad hoc network. It is essential that a wireless network should overcome the issue about physical medium, e.g., maximized bit rate, restricted range, noise, the minimal range of transmission, etc. As the nodes perform its mobility in the wireless ad hoc network, it is quite imperative that communication status and routing behavior will also change accordingly giving rise to dynamic topology. The presence of shared uncontained medium in a wireless network may also pose a significant security challenge while performing routing in the ad hoc environment [3]. Apart from this, energy has always been the peak problem associated with routing protocols in the wireless ad hoc network. Although there is various existing study to address such problem, the problems are not completely been solved. It is because usage of radio interfaces, directional antenna, and wireless technology are already shrouded with various security loopholes that are yet under the desk of researchers. The prominent attacks on the wireless ad hoc network are basically of two types, i.e., 1) routing-disruption attacks, and 2) resource-consumption attacks. The routing disruption-based attack is initiated by forwarding counterfeited beacon to mislead the route formation. Similarly, the resource-consumption based attack is responsible for initiating an attack that leads to unwanted drainage of energy or consumption of channel capacity. Although, the wireless ad hoc network uses both public and private key for performing encryption, usage of the public key is found more than private keys. This is because the implementation of the private key during distribution is quite difficult to be achieved in the presence of dynamic topology. There is another approach called Statistically Unique Cryptographically Verifiable (SUCV) that allows the nodes to select their addresses after generating public and private pairs of keys. However, this approach is found ineffective to address the problem of key set up [4]. Usage of Certificate Authority (CA) is another frequently used approach to secure the communication in the wireless ad hoc network. Therefore, there are multiple numbers of challenges being associated with the secure routing in the wireless ad hoc network. It is significantly felt that there is no efficient modeling for addressing secure routing issue. Study towards modeling will allow the system to evaluate the type of attackers as well as catch hold of the malicious node, which are very less being prioritized in existing techniques. Existing routing technique have proved potential improvement in security features but at the cost of computational complexity. Therefore, this paper discusses the three prominent forms of wireless ad hoc network i.e., mesh network, mobile ad hoc network, and vehicular ad hoc network. Although, wireless sensor network and delay tolerant protocol is also a significant form of ad hoc network, it has made some strong security implementation and is less considered when it comes to ad hoc environment. So, this manuscript doesn't discuss any research progress towards secure routing for wireless sensor network. Section II discusses security challenges followed by a discussion of existing techniques in Section III. Section IV discusses research gap while Section V briefs about the conclusion and tentative future direction of the research in secure routing in the wireless ad hoc network.

II. Security Challenges in Wireless Ad Hoc Network

The inherent characteristics of the wireless ad hoc network, itself, give rise to various forms of security challenges while performing routing operation. Some of the essential security challenges are as follows:

1) There is higher feasibility for a communication line to become victim of link attacks that could be in either of the form, i.e., messaging replay, impersonation, eavesdropping, etc. All these illegitimate operation offers a form of an access towards the confidential information. An intruder can directly corrupt the message or tamper the message using active attacks. All these adversarial operation leads to potential damage of integrity, availability, non-repudiation, and availability.

2) Normally, the nodes in wireless adhoc network don't have effective physical security that leads it to a very vulnerable condition in hostile environment. Hence, it is unwise to consider that origination of the intrusion could possibly happen from outside only. In order to maintain highest level of resiliency, ad hoc network are demanded to possess a distributed architecture without any central actor.

3) The wireless ad hoc network is also characterized by the dynamic topology that will mean that the nodes are performing, joining and leaving the defined network very frequently.

III. Secure Routing in Wireless Ad Hoc Network

A secure routing protocol over the wireless ad hoc network is not only meant for offering security features but also should keep communication performance in mind (Fig. 1). It has been seen that existing routing protocols can quite well cater up to the need of dynamic topology of ad hoc network, but they are highly incapable of resisting the malicious attacks.

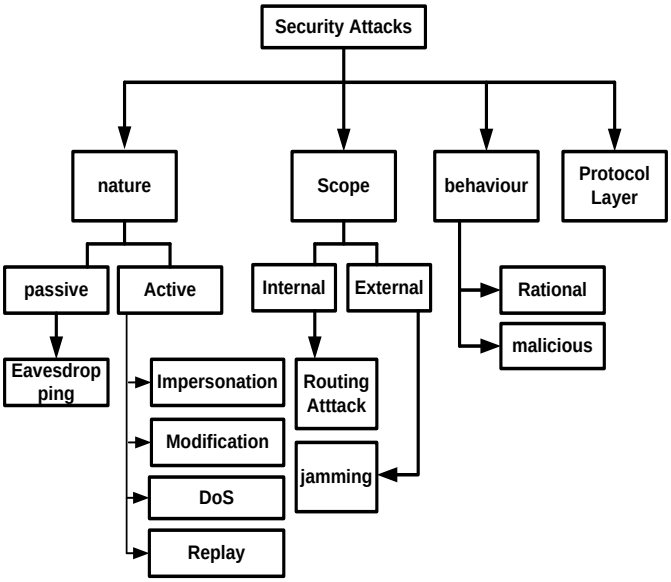

Fig. 1. Security intrusion in wireless ad hoc network.

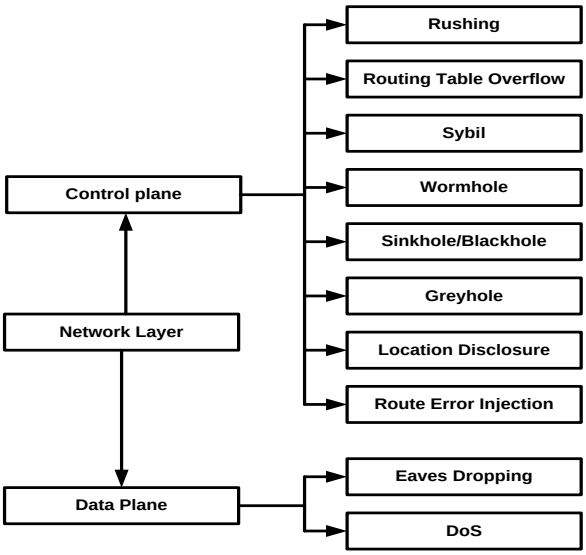

Fig. 2. Taxonomies of attacks on network layer

A closer look into the security attack taxonomies will show that there are essentially four types of intrusion in routing operation of wireless ad hoc network, i.e., attacks based on nature, attacks based on scope, behaviour-related attacks, and attacks on protocol layers. The frequently heard attacks of active and passive type come under nature-based attacks. Routing attacks come under internal attack while jamming attack comes under external attack. There are also behavioural-based attacks. The protocol layer-based attacks are classified depending on multiple layers, i.e., physical layer (jamming), MAC layer (flooding, MAC spoofing, replay attack), network layer (wormhole, control plane attack, sinkhole, blackhole, denial of service, eavesdropping), TCP layer (flooding and de-synchronization based attack). Attack associated with protocol layer particularly is more affected on network layer where the majority of the secure routing is implemented. Fig. 2 shows the taxonomies of attacks over network layer.

Basically, to resist such attacks, a secure routing protocol in the wireless ad hoc network is designed that are of two types: i.e., (1) *proactive* and (2) *reactive* form. *Secure Efficient Distance Vector Routing* (SEAD) [5] and *Secured Link State Protocol* (SLSP) [6] are two prominent protocols in proactive routing. SEAD is designed using destination sequence distance vector and is essentially meant for resisting jamming attacks, denial-of-service attacks, or any other forms of attacks that result in valuable resource consumption. The routing message is authenticated using the sequence number in SEAD. One of the major limitations of SEAD protocol is its dependencies of trusted entity that performs distribution of symmetric key in the network. Such phenomenon may give rise to bottleneck issue in the network. The next secured protocol SLSP is designed using link state protocol approach that aims to discover an effective topology followed by dissemination of packets of link state. It uses one-way hash function and neighbor lookup protocol for broadcasting state information. Unfortunately, SLSP is incapable of resisting colluding attacks, e.g., blackhole and wormhole attacks.

TABLE. I. CHARACTERISTICS OF SECURED ROUTING PROTOCOL

Protocol	Feature	Can resist	Cannot resist
SEAD	-Trusted Third Party (TTP) -Authentication using hop-by-hop -Hash function	-Rushing attack -Denial-of-Service	-Wormhole attack -Blackhole attack -Location disclosure
SLSP	-Threshold cryptography -Neighbour Lookup Protocol -Certification of Public keys by TTP	-Spoofing -Denial-of-Service	-Wormhole attack -Blackhole attack -Location disclosure
SAR	-Usage of different keys -Enhanced AODV implementation	-Rushing Attack -Routing Attack -Blackhole Attack	-Denial-of-Service -Wormhole Attack -Location disclosure
SRP	-Enhancement of Dynamic Source Routing -MAC is used for authentication Route Request and Route Reply	-Rushing Attack -Poisoning Attack -Routing Table Attack	-Denial-of-Service -Wormhole Attack -Location disclosure
SAODV	-Usage of Digital Signature -One-way Hash Chain -Enhancement of AODV	-Route Reply Attack -Rushing Attack -Replay Attack -Poisoning Attack -Routing Table Attack	-Denial-of-Service -Wormhole Attack -Blackhole Attack -Location disclosure
ARIADNE	-Secret Shared Key -Clock Synchronization -Authentication (end-to-end) -Dependency of key distribution center	-Selective Packet Dropping -Rushing Attack -Poisoning Attack -Routing Table Attack	-Denial-of-Service -Wormhole Attack -Blackhole Attack -Location disclosure
ARAN	-Uses TTP -Apriori secure link information among the nodes	-Spoofing -Rushing Attack -Illegitimate node participation	-Route Request Attack -Denial-of-Service -Flooding Attack -Wormhole Attack -Blackhole Attack
SEAODV	-Enhancement of AODV -Message Authentication (hop-by-hop) -Bloom's key	-Rushing Attack -Flooding Attack	-Denial-of-Service -Wormhole Attack -Blackhole Attack -Location disclosure

The reactive protocols make use of flooding of route request message and further classified into 6 types: i.e., 1) *Security-aware Ad hoc Routing* (SAR) [7], 2) *Secure Routing Protocol* (SRP) [8], 3) *Secure Ad hoc On-demand Distance Vector* (SAODV) [9], 4) *A Secure On-demand Routing Protocol for Ad hoc Network* (ARIADNE) [10], 5) *Authenticated Routing for Ad hoc Network* (ARAN) [11], and 6) *Secured Enhanced AODV* (SEAODV) [12]. The numbers of secure routing techniques are more in reactive form as compared to proactive form. Therefore, we briefly discuss its characteristics in Table 1.

There are also other forms of taxonomies of intrusion when it comes to secure routing protocol in the wireless ad hoc network. We find that design of secure routing is done by *prevention* and *identification* approach. Some good example prevention-based routing approaches are i) ARAN (using asymmetric cryptography), ii) SAR and SRP (using symmetric cryptography), iii) SEAD and ARIADNE (using one-way hash chain), iv) SLSP and SAODV (hybrid approach). Similarly, secure routing protocols based on identification are as follows e.g. i) Byzantine algorithm [13], ii) CORE algorithm [14], iii) CONFIDANT algorithm [13], and iv) WatchDog and Pathrater [15]. However, in the vehicular network, the trust factor is extensively used. The secure routing techniques in vehicular network consist of *infrastructure based* and *self-organizing based trust*. The majority of the existing secure routing protocols towards trust-based approaches mainly use precise location of the source, cryptographic authentication using public key infrastructure, repudiation of transmitter's identity, message transmission of other vehicular nodes, and validation of infrastructure. The existing techniques towards securing communication in the wireless ad hoc network mainly attempts to offer security toward the broadcasted information that bears sender's information during route discovery process. The routing techniques are also meant to provide identification of the type of attacks especially about the spoofed or forfeited information during ad hoc communication. A greedy-based technique is one of the frequently used in the wireless ad hoc network. However, apart from securing the communication link, these reported existing protocols are consistently used in research work by different forms. Still, the biggest hurdle is that they are not completely capable of mitigating denial-of-service, wormhole attack, blackhole attack, location disclosure attack, etc. The next section highlights some recent work carried out in the secure routing protocol.

IV. EXISTING TECHNIQUES OF SECURE ROUTING

Studies towards evolving up a secured routing mechanism in the wireless ad hoc network have various variations of techniques as well as approaches. The existing security techniques are designed for addressing explicit problems about security loopholes. We discuss only the significant research techniques published during 2010 to till date. For effective discussion, we brief the existing research contributions to different categories of the wireless ad hoc network below.

A. Studies in Wireless Mesh Network

A Wireless Mesh Network (WMN) is a type of ad hoc network where multiple nodes are connected to each other in a mesh topology. It is characterized by multiple communication paths to ensure zero link breakage as well as it also ensures highest link quality by minimizing the spatial distance among the nodes [16]. The best part is WMN can be combined with

existing standards, e.g., IEEE 802.15/16/11, sensor network, the internet, etc. to offer data communication service. However, WMN suffers from significant security problems on routing as it highly depends on adopting multicast routing schemes. Such schemes are never safe for active intrusions. Most recent, the work carried out by Matam and Tripathy [17] have used digital signatures for developing a secure routing mechanism to resist wormhole attack in WMN. The study outcome was compared with some of the conventional routing scheme to find better security performance. Another significant problem associated with WMN is involvement of multiple operators that results in zero cooperation finally leading to malicious behavior of a node. This problem has been addressed by Subhash and Ramachandram [18] who enhanced the feature of Ad hoc On-Demand Distance Vector (AODV) for constructing a trust and reputation model. The technique implements an algorithm to evaluate trust followed by recommendation of trust and selection of secured trusted path. The above-mentioned problems of multiple operator involvements also lead to intrusion of privacy in WMN as the attacks based on network layers are too high in it. This problem was found to be addressed by Meganathan and Palanichamy [19] who have used cross-layer approach with group signature scheme to resist such attacks. The technique also uses dynamic reputation for building subjective logic while performing route discovery in WMN. Adoption of the cross layer has been seen in the study of Bansal *et al.* [20] for developing a unique intrusion detection system. Such problems of intrusion can be counter-measured by including strong authentication protocol. Li *et al.* [21] have presented a public key encryption for enhancing the operability of Kerberos protocol by using arbitrary numbers. Hybridizing is another mechanism found out by certain researcher, e.g., Avule *et al.* [22] for strengthening security in WMN. This technique appends fields of message extension to the frame elements of selected route. The study outcome shows good communication performance for the smaller network. For the larger network, WMN uses hop-by-hop communication that is highly prone to cyber-attack. This problem was addressed by Gharavi and Hu [23] by using a dynamic update strategy towards the distribution of the secure key. The technique utilizes hash-based encryption to cipher the secure messages against Denial-of-Service attacks in WMN. There is already a default routing protocol in WMN that are found to be protected by various existing research-based secured routing technique. Tan *et al.* [24] have evaluated the strength of existing security approaches. The study outcome speaks of non-availability of robust security feature while routing in WMN.

B. Studies in Mobile Ad hoc Network

Mobile Ad hoc Network (MANET) is another type of wireless ad hoc network where each mobile node are also considered to be the router. It has highly decentralized architecture and characterized by dynamic topology. These inherent characteristics are itself possessed as a great security threat to its routing protocols. Although there are various existing studies towards secured routing in MANET [25], there is no single standard protocol being found 100% resilient against complex intrusion. In this regards, AODV is being used various researchers for incorporating security in MANET. Alkhamisi and Buhari [26] have enhanced the AODV by introducing multipath-based and trust-based communication in it. The technique is responsible for monitoring the communication behavior of a mobile node followed by computation of trust factor for identification of intrusion. Discussion of trust-model was also seen in the studies of Rikli and Alnasser [27] who have developed a centralized architecture to compute trust. Another bigger problem within MANET secure routing is the adoption of multicast communication strategy that drains high energy and overshoots delay and overheads. This problem was addressed by Madhusudhanan *et al.* [28] by introducing key management exclusively for multicast routing. This technique utilizes encryption techniques with the session key for forwarding the data using multicast routing over fixed interval for rekeying. Security problems about multicast routing in MANET have been addressed by Vijendran and Gripsy [29]. This technique assists in on-demand discovery. Multicast routing also leads the location information quite vulnerable in MANET. Research in this direction has been carried out by Saravanan and Sakthivel [30] who have used a digital signature with a time stamp for carrying out authentication. A private key crypto-system has been introduced with a symmetric key for ensuring sufficient privacy of location information in MANET. There are also schemes that perform repeated encryption process to resists attacks. One such scheme is found in the work of Wu *et al.* [31] where symmetric encryption is used without any need to change source node protocol. Sekaran and Parasuraman [32] have used Advanced Encryption Standard (AES) algorithm to secure communication while disseminating location information within it. The technique is resistive against any attack that causes depletion of the energy of the mobile node at any cause. Study towards addressing anonymity problems in communication for ad hoc network has been carried out by Yuan [33]. The technique renders all the communication nodes along with the intermediate node anonymous using the public key. The technique is found to be completely independent of any additional key establishments. Sagheer and Taher [34] have used identity-based encryption over AODV to offer secured routing. A similar form of study was also carried out by Wan *et al.* [35] where author have addressed the privacy problems as well as unlink ability issue in communication over MANET. The technique mainly uses identity-based encryption and group signature to retain potential privacy.

C. Studies in Vehicular Ad hoc Network

Vehicular Ad hoc Network (VANET) is another form of wireless ad hoc network that is characterized by infrastructure less and applies multihop network for providing communication. The study of VANET considers two forms of actors i.e. Road Side Unit (RSU) and On-Board Unit (OBU). A vehicle node is normally termed as OBU which has communicated with another OBU using RSU [36]. Hence, as faster security operations are required in VANET system that can normally be offered by Public Key Infrastructure (PKI). Unfortunately, these mechanism suffers from serious pitfalls, and hence it is not much applicable in VANET system (however, it is much better in another form of the wireless system e.g. wireless sensor network). Study on this direction was carried out by Tan *et al.* [37] by introducing a unique key management approach. The technique uses asymmetric

encryption mechanism for controlling the computational cost. The technique allows concatenating identity and its respective public key for OBU as well as RSU that results in the elimination of revocation list of certificates. Another key management strategy has been introduced by Vijayakumar *et al*. [38] that center around trusted authority to perform communication. The technique introduces a dual authentication approach for resisting illegitimate vehicular node from entering VANET system. Similarly, key management is also carried out using dual manner for effective dissemination of group key. The study contributes to cost-effective mechanism to add or revoke user in VANET. Study towards strengthening authentication mechanism is also discussed by Wang *et al*. [39] along with privacy problems. The technique uses biological password as well as decentralized digital certificate to perform authentication. In cryptography, ensuring fault tolerance is one of the challenging tasks especially in VANET system. Research towards implementing fault tolerant communication system has been carried out by Li *et al*. [40]. The author uses the Light Encryption Device (LED) principle that was originally implemented by Guo *et al*. [41]. The technique is claimed to support 64-128 bit encryption key that is similar to AES performance. Ultimately, the study finds the vulnerability factor of LED in VANET system. However, one of the biggest impediments towards VANET security is to even identify the extent of malicious information in dissemination process. A research attempt of Li and Song [42] has introduced a methodology using trust factor for identification of the malicious node as well as malicious data. Lo, and Tsai [43] have used Elliptical Curve Cryptography (ECC) as well as an identity-based signature mechanism to secure the communication system in VANET. The scheme mainly focuses on efficient authentication process between RSU and Vehicular nodes. Study towards group key dissemination scheme is presented by Park and Seo [44]. The technique constructs protocols for securing a vehicle to vehicle communication along with the assurance of system integrity. Tan *et al*. [45] have introduced filtering algorithm based on the fuzzy logic-based approach to computing the trust factor of a node in VANET. An interesting technique has been presented by Tripathi *et al*. [46] towards privacy problems in VANET system by incorporating private key encryption. Uniquely, the technique uses multilingual translation mechanism for encoding the messages. Yang *et al*. [47] have used reputation-based approach along with Dempster-Shafer evidence theory for identifying the selfish node. The technique is also found to address the energy problems too along with security features. Abumansoor and Boukerche [48] have addressed the security problem arising from the location of non-line of sight in VANET. The summary of the existing techniques to secure the wireless ad hoc network is sown below in Table 2.

TABLE. II. SUMMARY OF EXISTING TECHNIQUES TO SECURE WIRELESS AD HOC NETWORK

	Authors	Problems	Techniques	Contribution	Limitation
Wireless Mesh Network	Matam [17]	Wormhole attack	Digital signature	Resistive against routing loop attack, Route corruption attack, metric manipulation attack.	It doesn't offer faster response time for large network
	Subhash [18]	Node misbehaviour	Trust and reputation	Accurate trust recommendation	Trust model offer significant overhead
	Meganathan [19]	Network layer attacks	Cross layer, ID based encryption, group signature	Ensure privacy, security, reliability	Lower response rate, computational complex
	Bansal *et al*. [20]	Detection of malicious behaviour	Cross layer,	Resistive towards low intensity attack and can identify switching behaviour	Outcomes are not benchmarked
	Li *et al*. [21]	Authentication	Enhancing Kerberos protocol using public key cryptography	Public keys are kept separated from higher calculation of cost	No benchmarking of outcomes, less consideration of mobility.
	Avule *et al*. [22]	Security attacks	Adding fields to frames of selected path	Protect both mutable and non-mutable fields, good communication performance	Not applicable to large scale networks
	Gharavi [23]	Cyber-attack, denial-of-service	Hash based encryption	Simplified encryption technique	Only subjective to denial of service attack
	Tan *et al*. [24]	Comparative study of existing secure routing	Comparative analysis	Existing techniques are not robust	-
Mobile Ad hoc Network (MANET)	Alkhamisi [26]	Attack identification & isolation	Enhancing AODV, adding trust	Enhances throughput	Less effective benchmarking, behaviour to large & sparse network is not found
	Rikli [27]	Attack identification	Trust-based modeling	Claimed to detect all types of attackers	Recursive functions will lead to complexity and overhead It is subjective approach to sensor network only.

	Madhusudhanan *et al*. [28]	Security in multicast routing	Key management, fixed interval for rekeying, session key	Minimizes overhead of rekeying	Rekeying generates memory overflow in dense network
	Vijendran [29].	Security in multicast routing	Dynamic mobile point relay, location	Claimed to be energy efficient	Delay and overhead could possibly shoot up in real-time file transmission as well as in large network.
	Saravanan [30]	Privacy of location in multicasting, identity-spoofing attack	Symmetric key, digital signature	Ensure location anonymity	Not applicable for variable bit rate traffic, less evidence to prove key strength
	Wu *et al*. [31]	Routing attack	Double encryption	Have low complexity	Not applicable to variable bit rate traffic, not tested over large scale network.
	Sekaran [32]	Security and seamless communication	AES protocol	Good communication performance	Outcome is not benchmarked, algorithm complexity over not is not testified
	Yuan [33]	Packet analysis attack, anonymity problems of nodes, active attacks, denial-of-service	Public key encryption	Zero dependency of extra key establishment	Uses RSA
	Taher [34]	Security for nodes	Identity-based encryption	Simple technique	Not applicable for larger network with increased node mobility
	Wan *et al*. [35]	Anonymity	Identity-based encryption, group signature	Better packet delivery performance	Not applicable for larger network with increased node mobility
Vehicular Ad hoc Network (VANET)	Tan *et al*. [37]	PKI problems	Asymmetric encryption	Control computational cost, reduced time for key generation	High storage cost
	Vijayakumar *et al*. [38]	Authentication, key management	Fuzzy logic, dual approach for group keying and authentication	Computationally cost effective	Doesn't address node location privacy, constructed fuzzy rule-set cannot cover up entire dynamic scene of communication.
	Wang *et al*. [39]	Authentication, privacy	Biological password, decentralized certificate authority	Significant control over computational cost, minimizes overheads	Resilient to only denial-of-service
	Li *et al*. [40]	Assessing fault for LED	Mathematical analysis	Study finds LED to be vulnerable	Study focused on side-channel attack
	Li [42]	Identification of data trust	Trust management scheme	Better precision performance	Chances of increased overhead on large network
	Lo [43]	Privacy in VANET	Identity-based signature, ECC	Reduced time consumption	Iterative process will lead to space complexity
	Park [44]	Securing group communication	Constructed protocol to protect group key	Faster response time, scalable performance	Outcomes not benchmarked
	Tan *et al*. [45]	Attacks in data plane of VANET	Fuzzy logic	Detects and resist well for attacks in data plane	Constructed fuzzy rule-set cannot cover up entire dynamic scene of communication.
	Tripathi *et al*. [46]	Privacy in VANET	Multilingual translational	Very simple technique to implement	Not resistive against node capture attack or key compromise attack.
	Yang *et al*. [47]	Selfish node in VANET	Dempster Shafer, Reputation	Faster response time for decision making	Space complexity not addressed
	Abumansoor [48]	Security over non-line of sight	Collaborative protocol	Maintains integrity in localization services	Protocol doesn't work if there is no shared neighbor node.

V. RESEARCH GAP

From the previous section, it has been seen that there are various attempts being made towards addressing secure routing problems in the wireless ad hoc network. Table 1 has discussed the contribution along with limitations of each approaches being studied. There is no doubt that all the above-mentioned techniques have some significant contribution that assists the future researchers potentially; however, it cannot be ignored that each technique of existing literature is also associated with certain limitation. In this section, we will point out certain research gap, which we felt that it could have been addressed in the past but was not found so because of unknown reason. The significant research gaps are as follows:

A. Unbalanced Focus in Research Technique

It could be notably understood that there are discrete forms of secure routing techniques and trust/reputation-based approach is common to find in the wireless ad hoc network. The majority of the research using trust has used it only for choosing the secured route that is found matching with certain trust conditions. Unfortunately, such schemes are not found to balance the anticipated communication need (e.g., throughput) of a node in the generic environment of the wireless ad hoc network. Similarly, we also find that the methodologies of designing intrusion detection system are quite specific to a type of wireless ad hoc network that will mean its dependencies over the specific form of network. It will also mean that such scheme may be very particular to one type of wireless ad hoc network and cannot be exchanged with each other. This will pose a practical implementation of the wireless ad hoc network in real-time while working on the collaborative network. Another observation is that all the trust-based approaches have been remodeled and novelty is still missing. Hence, there is a need that such techniques should be seriously designed by re-defining the generic environment of the wireless ad hoc network.

B. Frequent Usage of AODV

The majority of the studies towards secure routing over the wireless ad hoc network is constructed on the top of frequently used AODV as routing protocol. Well, the problem is AODV suffers from the problem of stale data while routing and it can significantly generate control overhead. Existing study doesn't enhance AODV but just add security on the top of it that eventually means that still the legacy communication problems in a new protocol are allowed to be continued unnoticed. It was also known that usage of AODV or applying any form of remodeling it with sophisticate cryptography (e.g., hashing, ECC, symmetric encryption, etc.) will only lead to bandwidth consumption that has never been found to be testified while evaluating security strength in the existing system. There is far better and efficient routing protocol in wireless ad hoc network, e.g., Optimized Link State Routing (OLSR) which could also be used in secure routing. However, the trend is more on AODV while implying security features.

C. Missing Feature in Attack Identification and Isolation Techniques

Maximum category of the existing literature is focused on using the principle of attack identification and isolation. However, we find that such schemes are all focused on particular types of attack and that will mean that they are not capable of resisting another form of attack. The second problem in all these approaches is that they consider single intruders while routing and so existing system fails to address the security breach problem that may occur in the presence of dual colluding intruders. The third potential problem in this regard is that all the cryptographic based approach are shown to have a successful outcome when it comes to identification of attacks. However, there are no significant studies where the malicious nodes have been identified effectively. Certain studies which introduces selfish node may turn out to be regular node after accomplishing its objective, and hence existing techniques fails to discretize the form of attack while constructing the secure routing principle.

D. Less Focus on Computational Complexity

Existing techniques using digital signatures can potentially lead to communication overhead and possibly invite other forms of attack, which they are not meant to resist. The process of signing the message involves computational cost that may increase exponentially with increase in network sizes. There is also a possibility of lack of spontaneous network as such technique will require nodes to have apriori information about each other for facilitating sharing of public keys.

E. No Significant Initiative towards Optimization

We find that cost-effective optimization process is not being incorporated in the existing research techniques towards securing routing in the wireless ad hoc network. Without optimization technique, it is quite impossible for cost effectively plan the equilibrium between security computation and communication performance under any adverse scenario of intrusion. Hence, there is an emergent need for such research direction.

VI. CONCLUSION & FUTURE WORK

According to the theory, the wireless ad hoc network is one of the best alternative ways to establish connectivity in the region which doesn't have any form of infrastructure. However, establishing communication among the nodes is not that easy task in the ad hoc network as these nodes are consistently moving and forming a dynamic topology. The conventional study says that in MANET and rural VANET system, the node could move in any arbitrary direction; however, in the case of urban VANET system the path is very well defined. All this will mean that the applicability of the routing protocols in wireless ad hoc network differs in different forms of the network. This pattern is also same for secure routing protocols. First of all, there is extremely less progress made towards evolving up with secure routing techniques in the wireless ad hoc network, and the only handful of names of routing protocol exists in present time. This document has reviewed some of the recently implemented routing protocols to mitigate attacks in the wireless mesh network, mobile ad hoc network, and vehicular ad hoc network. We also find that there is significant research gap explored from existing literature, e.g., unbalanced focus in research technique, frequent usage of AODV, missing a feature in attack identification and isolation techniques, less focus on computational complexity, no

significant initiative towards optimization. So, our future work direction will be towards addressing such explored problems.

Our first initiative toward future research work will be to develop a secure routing protocol to address some lethal attacks. This review finding suggests that certain lethal attacks, e.g., wormhole attack, black hole attack, location disclosure, and denial-of-service are rarely addressed by existing secured routing techniques. Our future idea will be to evolve up with an analytical modeling that formulates a virtual decoy node to capture the attacker as well as isolate the attacker. A novel adversarial model will be designed based on the features of above-mentioned attacks. Our second research initiative will also be to explore the feasibility of coming up with cost effective optimization model as it is quite a few to find in existing literature.

REFERENCES

[1] N. Chaki, R. Chaki, "Intrusion Detection in Wireless Ad-Hoc Networks", CRC Press, pp. 258, 2014

[2] M.A. Matin, "Handbook of Research on Progressive Trends in Wireless Communications and Networking", IGI Global, pp. 592, 2014

[3] S. Khan, J.L. Mauri, "Security for Multihop Wireless Networks", CRC Press, pp. 538, 2016

[4] F. Anjum, P. Mouchtaris, "Security for Wireless Ad Hoc Networks", John Wiley & Sons, pp.316, 2007

[5] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, USA, pp. 3 – 13, 2002

[6] P. Papadimitratos and Z. J. Hass, "Secure link state routing for mobile ad hoc networks", In Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), pp.379-383, Washington DC, USA, 2003

[7] S. Yi, P. Naldurg and R. Kravets, "Security-aware ad hoc routing for wireless networks", Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'01), Long Beach, CL, USA, pp.299 – 302, 2001

[8] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'02), San Antonio, TX, USA, pp. 27-31, 2002

[9] M. G. Zapata and N. Asokan. "Securing ad hoc routing protocols", In Proceedings of the 1st ACM Workshop on Wireless Security, Atlanta, GA, USA, pp. 1-10, 2002

[10] Y.-C. Hu, A, Perrig, and D. Johnson, " Ariadne: a secure on-demand routing protocol for ad hoc networks", In Proceedings of ACM Annual International Conference on Mobile Computing (MobiCom'02), Atlanta, GA, USA, pp. 21 – 38, 2002

[11] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, pp. 78 – 87, 2002

[12] C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks", International Journal of Network Security, vol 13, no 2, pp. 109-120, 2011

[13] M. Yu, M. Zhou and W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," in IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-460, 2009.

[14] P. Tomar, P.K. Suri, M.K. Soni, "A Comparative Study for Secure Routing in MANET", International Journal of Computer Applications, Vol.4(5), pp.17-22, 2010

[15] "Chapter 11 Detecting Bad Behaviors", http://perso.crans.org/raffo/papers/phdthesis/thesisch11.html, Retrieved 16th June-2017

[16] S. Misra, S.C.Misra, I.Zhang, "Guide to Wireless Mesh Networks", Springer Science & Business Media, pp.528, 2009

[17] R. Matam and S. Tripathy, "Secure Multicast Routing Algorithm for Wireless Mesh Networks", Journal of Computer Networks and Communications, pp.11, 2016

[18] P. Subhash and S. Ramachandram, "Trust Based HWMP Protocol in High-Performance Wireless Mesh Networks", work, vol.5(6), pp. 11-25, 2016

[19] N.T. Meganathan and Y. Palanichamy, "Privacy Preserved and Secured Reliable Routing Protocol for Wireless Mesh Networks", The Scientific World Journal, pp.12, 2015

[20] D. Bansal, S. Sofat and P. Kumar, "Distributed cross layer approach for detecting multilayer attacks in wireless multi-hop networks," *2011 IEEE Symposium on Computers & Informatics*, Kuala Lumpur, pp. 692-698, 2011

[21] M. Li, X. Lv, W. Song, W. Zhou, R. Qi, and H. Su, "A novel identity authentication scheme of wireless mesh network based on improved kerberos protocol", In Distributed Computing and Applications to Business, Engineering and Science (DCABES), 13th International Symposium, pp. 190-194, 2014.

[22] M. Avula, S-G. Lee, and S-M. Yoo, "Security Framework for Hybrid Wireless Mesh Protocol in Wireless Mesh Networks", TIIS, vol. 8, no. 6, pp.1982-2004, 2014

[23] H. Gharavi and B. Hu, "4-way handshaking protection for wireless mesh network security in smart grid", In Global Communications Conference (GLOBECOM), pp. 790-795, 2013

[24] W.K. Tan, S-G. Lee, J.H. Lam, and S-M. Yoo, "A security analysis of the 802.11 s wireless mesh network routing protocol and its secure routing protocol" Sensors, vol. 13, no. 9, pp.1553-11585, 2013

[25] J. Loo, J.L.Mauri, J. H.Ortiz, "Mobile Ad Hoc Networks: Current Status and Future Trends", CRC Press, pp.538, 2016

[26] A. O. Alkhamisi and S. M. Buhari, "Trusted Secure Adhoc On-demand Multipath Distance Vector Routing in MANET," *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Crans-Montana, pp. 212-219, 2016

[27] R. Nasser-Eddine, and A. Alnasser, "Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks", International Journal of Distributed Sensor Networks, Vol. 12, no. 7, pp.1-16, 2016

[28] B. Madhusudhanan, S. Chitra, and C. Rajan, "Mobility based key management technique for multicast security in mobile ad hoc networks," The Scientific World Journal, pp.10, 2015

[29] A.S. Vijendran and J. V. Gripsy, "Enhanced secure multipath routing scheme in mobile adhoc and sensor networks", In Current Trends in Engineering and Technology (ICCTET), 2nd International Conference, pp. 210-215, 2014.

[30] T.R. Saravanan, and P. Sakthivel, "Location privacy protection for secure multicasting in MANET", In Recent Advances in Electronics & Computer Engineering (RAECE), National Conference, pp. 59-64, 2015

[31] X. Wu, X. Zhu and F. Kong, "Routing and Data Security Scheme Based on Double Encryption in Mobile Ad Hoc Networks," *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, Qinhuangdao, pp. 1787-1791, 2015

[32] R. Sekaran and G.K. Parasuraman, "A Secure 3-Way Routing Protocols for Intermittently Connected Mobile Ad Hoc Networks", The Scientific World Journal, pp.13, 2014

[33] W. Yuan, "An anonymous routing protocol with authenticated key establishment in wireless ad hoc networks", International Journal of Distributed Sensor Networks, pp. 10, 2014

[34] A.M. Sagheer and H. M. Taher, "Identity Based Cryptography for secure AODV routing protocol", In Telecommunications Forum (TELFOR), 2012 20th, pp. 198-201, 2012

[35] Z. Wan, K. Ren and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks," in *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1922-1932, May 2012.

[36] Al-S.K.Pathan, "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET", CRC Press, pp. 638, 2016

[37] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang and P. H. J. Chong, "A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9570-9584, 2016.

[38] P. Vijayakumar, M. Azees, A. Kannan and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015-1028, 2016

[39] F. Wang, Y. Xu, H. Zhang, Y. Zhang and L. Zhu, "2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896-911, 2016.

[40] W. Li, W. Zhang, D. Gu, Y. Tao, Z. Zhao, Z. Liu, "Impossible Differential Fault Analysis on the LED Lightweight Cryptosystem in the Vehicular Ad-Hoc Networks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 84-92, 2016.

[41] J. Guo, T. Peyrin, A. Poschmann and M. Robshaw, "The LED Block Cipher", Springer, pp. 326-341, 2011

[42] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960-969, 2016.

[43] N. W. Lo and J. L. Tsai, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319-1328, 2016.

[44] Y. H. Park and S. W. Seo, "Fast and Secure Group Key Dissemination Scheme for Out-of-Range V2I Communication," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5642-5652, 2015.

[45] S. Tan, X. Li and Q. Dong, "A Trust Management System for Securing Data Plane of Ad-Hoc Networks," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7579-7592, 2016.

[46] V. K. Tripathi and S. Venkaeswari, "Secure communication with privacy preservation in VANET- using multilingual translation," *2015 Global Conference on Communication Technologies (GCCT)*, Thuckalay, pp. 125-127, 2015

[47] Y. Yang, Z. Gao, X. Qiu, Q. Liu, Y. Hao, and J. Zheng, "A hierarchical reputation evidence decision system in VANETs", International Journal of Distributed Sensor Networks, pp.4, 2015

[48] O. Abumansoor and A. Boukerche, "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET," in *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275-285, Jan. 2012

AUTHOR'S PROFILE

Jyoti Neeli, is currently a research scholar in RV College of Engineering, Bengaluru working as an Associate Professor in Department of Information Science & Engineering Global Academy of Technology, Bengaluru. She has completed her M. Tech in Computer Science & Engineering from VTU. She has 15 years of experience in teaching and 6 years in R&D. Her area of interest includes Computer networks, Software testing, Mathematical models.

Dr. N K Cauvery, is Professor and Head of Department of Information Science & Engineering, RV College of Engineering, Bengaluru. She has completed her Ph. D from VTU with research title as *"Routing in Computer Network using Genetic Algorithm".* She has 17 years of experience in teaching and 7 years in R&D. She has published papers both in national & international conferences. Her area of interest includes Computer network, Compiler Design, Genetic Algorithm.