International Journal of Security and Its Applications
Vol. 12, No. 2 (2018), pp.67-78
http://dx.doi.org/10.14257/ijsia.2018.12.2.06

A Detailed Review on Mobile Ad Hoc Networks: Protocols, Security Issues and Challenges

N. Thirupathi Rao[1], Pilla Srinivas[1], Debnath Bhattacharyya[1] and Tai-hoon Kim[2*]

[1]Department of Computer Science & Engineering
Vignan's Institute of Information Technology (A)
Visakhapatnam, AP, India
[2]Sungshin Women's University, Bomun-ro 34da-gil, Seongbuk-gu, Seoul, Korea
nakkathiru@gmail.com, debnathb@gmail.com,
**taihoonn@daum.net*

Abstract

In this article, an overview of secure specially appointed steering conventions for remote systems was presented. Impromptu system is a gathering of hubs that is associated through a remote medium framing quickly evolving topologies. Assaults on specially appointed system steering conventions disturb organize execution and unwavering quality with their arrangement. We quickly exhibit the most well-known conventions that take after the table-driven and the source-started on-request approaches. The associationflanked by the proposed arrangements and parameters of specially appointed system demonstrates the execution as indicated by secure conventions. We talk about in this paper directing convention and challenges and furthermore examine verification in specially appointed system.

Keywords*: Routing Protocols, Network security, security issues, Ad hoc Network, safetyrepair, Wireless Network, Routing Authentication*

1. Introduction

Wireless networks [4] comprise of various hubs which speak with each other over a remote station which have different kinds of systems: sensor arrange, specially appointed versatile systems, cell systems and satellite systems. Remote sensor systems include of smallcenter with detecting, calculation and remote interchanges capacities. Specially appointed systems are another worldview of remote correspondence for portable hosts where hub versatility causes visit changes in topology. Specially appointed systems are self-configurable and self-governing frameworks comprising of switches and has, which can bolster movablity and arrange themselves discretionarily. This implies the topology of the impromptu system changes progressively and unusually. In addition, the impromptu system can be either developed or destructed rapidly and self-rulingly with no managerial server or framework. Without help from the settled framework, it is without a doubt exhausting for individuals to recognize the insider and untouchable of the remote system. In other words, it is difficult for us to distinguish the legitimate and the illicit members in remote frameworks. Due to the previously mentioned properties, the execution of security foundation has turned into a basic test when we outline a remote system framework. On the off chance that the hubs of

Received (November 23, 2017), Review Result (February 28, 2018), Accepted (March 6, 2018)
* Corresponding Author

ISSN: 1738-9976 IJSIA

impromptu systems are portable and with remote correspondence to keep up the availability, it is known as versatile specially appointed system (MANET) and require a greatly adaptable innovation for building up interchanges in circumstances which request a completely decentralized system with no settled base stations, for example, war zones, military applications, and other crisis and fiasco circumstances.

In MANETs, every one of the hubs impart over remote connections with no settled foundation. MANETs are appropriate to situations in which there is no settled framework or when the foundation isn't trusted. In such systems, a typical methodology is to shape bunches where every hub is connected to a group set out toward proficient steering with different hubs that are not in its immediate range. GAs have been utilized as a part of such bunch based steering plans for MANETs. Al Gazal *et al.* [4] have proposed a GA-based convention named 'group portal switch steering convention' (CGSRP) to choose the bunch take to take away correspondence between hubs. Group head must have enough assets, power, and data transfer capacity to keep away from threats of bottlenecks. This plan works by encoding every hub's one of a kind ID in the chromosomes. The chromosomes have data about group head, individuals, number of connections in each bunch head. The encoded chromosomes are then assessed against specific criteria as characterized by the wellness work (which may join highlights, for example, stack adjusting and data transfer capacity protection). Every chromosome's wellness is then assessed. The procedure of the survival of the fittest prompts an ideal choice of hubs as bunch heads that ideally use assets.

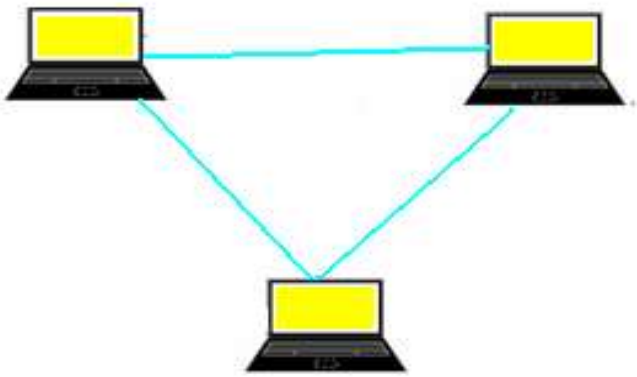

Figure 1. Network Model

Since all hubs are portable, the system topology of a MANET is by and large powerful and may change every now and again. In this way, convention, for example, 802.11 to convey by means of same recurrence or Bluetooth have required control utilization is specifically relative to the separation between single-jump transmissions [4]. To stay away from this steering issue, two hosts can utilize multi-bounce [34] transmission to convey through different has in the system A switch ought to give the capacity to rank directing data sources from most dependable to minimum reliable and to acknowledge steering data about a specific goal from the most reliable sources first. A switch ought to give an instrument to sift through clearly invalid courses. Switches must not naturally redistribute directing information they don't themselves utilize, trust or generally think about legitimate. Switches must be no less than a little neurotic about tolerating steering information from anybody, and must be particularly watchful when they circulate directing data gave to them by another gathering. Figure 1 demonstrates three hubs where impromptu system where each hub is associated with remote, and work as entréesummit to onward and obtaindata. The current review article talks

about assaults on specially appointed systems and examines current methodologies for building up cryptographic keys in impromptu systems. We portray the condition of research in secure specially appointed steering conventions, directing difficulties and its exploration issues.

A portion of the issues identified with remote correspondence are multipath spread, way misfortune, impedance, and constrained recurrence range. Multipath Propagation is, the point at which a flag makes a trip from its source to goal, in the middle of there are impediments which influence the flag to proliferate in ways past the immediate viewable pathway. Way misfortune is the lessening of the transmitted flag quality as it spreads from the sender. Way misfortune can be resolved as the proportion flanked by the forces of the transmitted flag to the recipient flag. This is primarily subject to various factors, for example, radio recurrence and the idea of the territory. It is some of the time imperative to evaluate the way misfortune in remote correspondence systems. Because of the radio recurrence and the idea of the landscape are not same all over the place, it is difficult to appraise the way misfortune amid correspondence. Amid correspondence various flags in the air may meddle with each other bringing about the devastation of the first flag. Constrained Frequency Spectrum is the place, recurrence groups are shared by numerous remote advances and not by one single remote innovation.

2. Routing.

In the midst of this method of routing, no short of what one widely appealing center point inside the web work is experienced. This thought isn't new to programming designing since controlling was used as a piece of the frameworks in mid 1970's. Be that as it may, this thought has achieved predominance from the 1980's. Regardless, at the present summit of the line and wide level internetworking has ended up being outstanding with the latest types of progress in the frameworks and media transmission advancement. The coordinating thought basically incorporates, two activities: immediately, choosing perfect controlling ways and moreover, trading the information social occasionsthrough an internetwork. The later thought is called as bundle trading which is straight forward, and the way confirmation could be amazingly complex[4]. Guiding traditions use a couple of estimations to figure the most ideal approach to defeat the groups to its objective.

This course information changes beginning with one directing computation then onto the following. Guiding tables are stacked with a collection of information which is made by the coordinating counts. Most consistent sections in the coordinating table are ip-address prefix and the accompanying skip. Controlling table's Destination/next hop affiliations tell the switch that a particular objective can be come to in a perfect world by sending the package to a change addressing the "accompanying skip" on its way to the last objective and ip-address prefix shows a course of action of objectives for which the coordinating area is true blue for. Trading is by and large direct differentiated and the way affirmation. Exchanging takes after, a host chooses like it should send some package to another host. By a couple of means it picks up the switches address and sends the bundle had a tendency to expressly to the switches MAC address, with the tradition address of the objective have.

Coordinating is generally orchestrated into static controlling and dynamic coordinating. Static guiding implies the coordinating framework being communicated physically or statically, in the switch. Static controlling keeps up a coordinating table by and large created by a frameworks chief. The coordinating table doesn't depend upon the state of the framework status, *i.e.*, paying little mind to whether the objective is dynamic or not [6]. Dynamic guiding insinuates the coordinating philosophy that is being learnt by an inside or outside directing

tradition. This guiding generally depends upon the state of the framework *i.e.*, the directing table is impacted by the movement of the objective. The genuine insult with static coordinating is that if another switch is incorporated or ousted in the framework then it is the commitment of the administrator to reveal the key changes in the guiding tables. Be that as it may, this isn't the circumstance with dynamic directing as each switch announces its quality by flooding the information package in the framework so every switch inside the framework get some answers concerning the as of late included or cleared switch and its doors. Also this is the same with the framework parcels in the dynamic guiding [3].

3. Categorization of Routing Protocols.

We will look at the request of existing remote adhoc directing traditions, their trademark features and sorts. The Routing Protocols for extraordinarily designated remote frameworks can be parceled into three classes in perspective of the guiding information revive framework. This isn't the circumstance, in any case, for on-ask for coordinating traditions. Right when a center using an on-ask for tradition needs a course to another objective, it should hold up until such a course can be found. Of course, because coordinating information is consistently multiplied and kept up in table-driven directing traditions, a course to each other center point in the improvised framework is continually open, paying little personality to paying little respect to whether it is required [10]. In this paper we have presented an essential examination of the already said secure directing traditions. To begin with we display an examination between the two wide classes of controlling traditions in perspective of their coordinating framework and other framework parameters.

3.1. Proactive Protocols

These traditions constantly keep up in the current style information of courses from each center to each other center point in the framework. In this way, when there is a prerequisite for a course to an objective, such course information is open rapidly. Particular traditions screen various coordinating state information [11]. These traditions require each center point to keep up no less than one tables to shroud away to date guiding information and to spread updates all through the framework. In like manner, these traditions are consistently furthermore suggested as table-driven. These traditions endeavor and keep up generous courses to all correspondence adaptable center points always, which infers before a course is extremely required. Incidental course invigorates are exchanged with a particular ultimate objective to synchronize the tables.

3.1.1. DSDV

Routing convention remains contingent on the opportunity of the well-known Bellman-Ford Routing Algorithm with preciseimprovements, for example, influencing it to circle free. The separation vector steering is less vigorous than interface state directing because of issues, for example, tally to limitlessness and skipping impact. In this, every gadget keeps up a directing table containing passages for every one of the gadgets in the system. To keep the directing table totally refreshed at all the time every gadget intermittently communicates steering message to its neighbor gadgets. At the point when a neighbor gadget gets the communicated directing message and knows the present connection cost to thegadget, it thinks about this esteem and the relating esteem put away in its directing table. On the off chance that progressions were discovered, it refreshes the esteem and re-processes the separation of the course whichincorporates this connection in the steering table.

3.2. Reactive Protocols.

The responsive or on-ask for directing traditions rely upon Query-Reply topology in which they don't try to constantly keep up the front line topology of the framework. Exactly when a course is needed, a strategy is summoned to find a course to the objective center point. The genuine target of on asks for or open coordinating traditions are to constrain the framework movement overhead. These controlling traditions rely upon some sort of "question reply" trade. They don't try to reliably keep up the cutting edge topology of the framework. Or then again perhaps, when the need develops, a responsive tradition summons a framework to find a course to the objective; such a strategy incorporates a kind of flooding the framework with the course question. As needs be, such traditions are as often as possible moreover implied as on ask. The fundamental part in responsive traditions is the instrument used for discovering courses. The source center transmits a request message, requesting a course to the objective center point. This message is flooded, *i.e.* exchanged by all center points in the framework, until the point that it accomplishes the objective. Along these lines diverse answer messages may come to fruition, yielding different courses - of which the most concise is to be used [24].

3.2.1. TORA

This protocol was created by Park and Corson. Incidentally requested steering calculation (TORA) is very versatile, circle free, circulated directing calculation in view of the idea of connection inversion. It utilizes coordinated non-cyclic diagrams to characterize the courses either as upstream or downstream. This diagram empowers TORA to give better course help to systems with thick, huge populace of hubs [28]. However to givethis component TORA needs synchronization of the hubs which constrains the use of the convention. TORA is a genuinely convoluted convention yet what makes it one of a kind and unmistakable is its fundamental component of proliferation of control messages just around the purpose of disappointment when a connection disappointment happens. In correlation, the various conventions need to re-start a course disclosure when a connection flops however TORA would have the capacity to fix itself up around the purpose of disappointment. This element enables TORA to scale up to bigger systems yet has higher overhead for littler systems. TORA includes four noteworthy capacities: making, keeping up, deleting and improving courses. Since each hub must have tallness, any hub which does not have a stature is considered as a deleted hub and its stature is considered as invalid. Here and there the hubs are given new statures to enhance the connecting structure. This capacity is called enhancement of courses.

3.2.2. DSR

DSR is a responsive convention *i.e.* it doesn't utilize occasional updates. It figures the courses when essential and after that looks after them. Source steering is a directing system in which the sender of a parcel decides the entire succession of hubs through which the bundle needs to pass, the sender unequivocally records this course in the parcel's header, recognizing each sending "bounce" by the address of the following hub to which to transmit the bundle on its way to the goal have. There are two fundamental parts of DSR convention: course disclosure and course upkeep. Each hub keeps up a reserve to store as of late found ways. At the point when a hub needs to send a parcel, it first checks the store whether there is a section for that. In the event that yes then it utilizes thatway to transmit the parcel. Likewise it joins its source address on the parcel. In the event that there is no section in the store or the passage is terminated, the sender communicates a course ask for bundle to every one of its neighbors

requesting a way to the goal. Until the point when the course is found, the sender haspauses. At the point when the course asks for bundle touches base to some other hubs, they check whether they know the goal inquired. On the off chance that they have course data, they send back a course answer parcel to the goal. Else they communicate a similar course ask for parcel. Once the course is found, the sender will send its required bundles utilizing the found course and additionally embed a passage in the store for sometime later. Additionally the hub keeps the age data of the passage to perceive whether the store is new or not. At the point when any transitional hub gets an information bundle, it first observes whether the parcel is sent to itself or not. In the event that it is the goal, it gets that else it advances the parcel utilizing the way appended on the bundle.

4. Safetyconfront in Ad Hoc Networks.

Utilization of remote connections renders an Ad hoc organize defenseless to interface assaults extending from inactive spying to dynamic pantomime, message replay and message bending [9],[10],[5].Eavesdropping may give an assailant access to mystery data in this way disregardingprivacy. Dynamic assaults could go from erasing messages, infusing wrong messages; imitate a hub and so on in this way disregarding accessibility, trustworthiness, verification and nonrepudiation. Hubs meandering uninhibitedly in an unfriendly domain with moderately poor physical security have non-unimportant likelihood of being bargained. Consequently, we have to consider malevolent assaults from outside as well as from inside the system from traded off hubs. In this way following are the routes by which security can be broken. [6]

a. **Channel Weakness:** Communications can be listened in and counterfeit communications can be infused into the system without the trouble of takingcorporaladmittance to arrange parts.
b. **Vulnerability of hubs:**Due to the system hubs for the most part don't do well in physically secured places, for example, bolted rooms, they would more be able to effectively be caught and dropbeneath the manager of an aggressor.
c. **Lack of Communications:** Ad hoc arranges should work autonomously of any settled foundation. This makes the traditional safetypreparations in view of confirmationspecialist and other regular hubs and machine servers inapplicable.
d. **With dynamic alteringof Topology:** In portable specially appointed systems, the perpetual modify of topology need advanced steering conventions the defense of which is an extra test. A specific trouble is that inaccurate directing data can be produced by traded off hubs or because of a number of topology alterations and it is difficult to recognize the binarygears.Ad hoc systems ought to have a conveyed engineering with no focalelements, centrality expands weakness for getting high availability. Specially appointed system is dynamic because of incessant changes in topology. Indeed, even the trust connections among singular hubs additionally changes, particularly when a few hubs are observed to be traded off. Security component should present on the lively ought to be adaptable.

5. Safety Form

In the current section, the discussion about safety objective assaults and thus protectedsteeringprotocol which can be discussed in the following as follows,

5.1. Safety Goals for Ad Hoc

a. **Availability:** In spite of Rejection of Provisionassaults,on physical also that media get to control layer assailant can utilize sticking strategies to meddle withCorrespondence on physical channel.
b. **Privacy:**Assurancesfirmstatistics is not ever uncovered to unapproved elements.
c. **Reliability:**Communicationactualitycommunicated is certainly not ruined.
d. **Confirmation:**Authorizes a center to assurance the charm of the subordinatecenter it is dialogue with.
e. **Non-revocation:**Guarantees that the beginning of a communication can't deny having sent the message.
f. **Non-pantomime:** No one else can profess to be another approved part to take in any valuable data.
g. **Assault utilizing creation:** Generation of false directing messages is named as manufacture messages. Such assaults are hard to identify.

6. Assaults on Ad Hoc Network

There are numerouskinds of outbreaks on ad hoc system which were discussed in detail in the following,

a. **PositionExpose:** Location confession is an attack that objectives the safety necessities of a particularlyselectedscheme. Using activity investigation systems [20], orwith more straightforward examining and checking approaches.
b. **Black Hole:** In a dark opening assault a pernicious hub pervadesincorrectsequenceresponses to the course demands it gets, endorsing itself as consuming the most brief way to a destination[6].
c. **Repetition:** An invader that plays out a repetition assault infuses into the schemeleadingmovement that has remainedwedgedpreviously.
d. **Blackmail:** This stabbing is applicable against directing resolutions that application instruments for the recognizable proof of noxious hubs and spread messages that endeavor to boycott the wrongdoer [8]. The security property of non-revocation can end up being helpful in such cases since it ties a hub to the messages it produced.
e. **Disowning of Facility:**Disowning of administration assaults go for the total disturbance of the directing work and in this way the whole task of the impromptu system [15]. Particular examples of dissent of administration assaults incorporate the directing table flood and the lack of sleep torment.
f. **Routing Table Poisoning:** For instance, an aggressor can send steering refreshes that don't compare to real changes in the topology of the specially appointed system.
g. **Rushing Attack:** For instance, DSR, AODV, what's more, secure conventions in light of them, for example, Ariadne, ARAN, and SAODV, can't to find courses longer than two jumps when subject to this assault. create Rushing Assault Prevention (RAP), a bland guard against the surging assault for on-request conventions that can be connected to any current on-request directing convention to permit that convention to oppose the hurrying assault.
h. **Breaking the neighbor relationship:** A canny channel is set by a gatecrasher on a correspondence interface between two ISs(Information framework) could adjust or change data in the steering refreshes or even capture movement having a place with any information session.

i. **Passive Listening and movement investigation:** The interloper could latently accumulate uncovered directing data. Such an assault can't impact the activity of directing convention, yet it is a rupture of client trust to steering the convention. Hence, touchy directing data ought to be secured. Be that as it may, the classification of client information isn't the duty of steering convention.

7. Routing safety in Ad Hoc Network

The contemporary steering conventions for Ad hoc organizes adapt well to progressively changing topology yet are not intended to suit safeguard against noxious assailants. No single standard conventions catch normal security dangers and give rules to secure directing. Switches trade arrange topology casually another potential focus for pernicious aggressors who plan to cut down the system. Outside aggressors infusing wrong directing information, replaying old steering data or contorting directing data keeping in mind the end goal to segment a system or over-burdening a system with retransmissions and wasteful steering. Inner traded off hubs - more extreme location and rectification more troublesome Routing data marked by every hub won't work since bargained hubs can produce substantial marks utilizing their private keys. Discovery of traded off hubs through steering data is additionally troublesome because of dynamic topology of Ad hoc organizes [22]. Steering conventions for Ad hoc organizes must deal with obsolete directing data to suit dynamic evolving topology. This however needs the presence of numerous, perhaps disjoint courses between hubs. Steering convention ought to have the capacity to make utilization of a backup way to go if the current one seems to have blamed.

7.1. Fresh Key Assertion Situation

They believe each other by and by; however don't have any from the earlier shared mystery (watchword) to verify each other. They don't need anyone outside the space to get a breeze of their discussion inside. This specific situation is defenseless against any aggressor who can screen the correspondence as well as alter the messages and can likewise embed messages and influence them to seem to have originated from someone inside the room [10].

7.2. Two Evident Issues

Difficult to decide whether the declaration exhibited by the member has been denied participants might be partitioned into at least 2 accreditation progressive systems and that they don't havecross confirmation chains of command. One clear arrangement.Actuallyprotectedconduit constrained to those there in the space to arrange the sittingenterearlier than changing to the shaky remote conduit.

7.3. Secret Word Bottomauthenticinputswap

A new watchword is picked with a specific end goal to catch the current shared setting. On the off chance that this secret key is long irregular string, can be utilized to setup security affiliation, yet less easy to use. Normal dialect phrases are more clients benevolent, however helpless against word reference attacks [10][6][4]. Need to determine a solid sittinginput from a powerless shared secret word. Attractive properties for such a convention are following,

a. **Privacy:**Simply that group of actors that make out the underlying communal powerless mystery watchword ought totake in the sittinginput and no one else should.

b. **Idealonwardconfidentiality:**An aggressor who prevails with regards to trading offone of the members at a later time would be notable make sense of the session key coming about because of past keeps running of convention.
c. **Contributory Key Agreement:** If every single player takes an interest in the production ofthe last sittinginput, by considering a commitment, at that point it is known as contributory key assertion.
d. **Acceptance to disturbanceefforts:**Solid aggressors not only who can disturb correspondence by sticking radio channels and so on yet even the weaker assailants who canembed however can't change or erase messages sent by players are likewise accommodated.

7.4. Assessment of Safe Protocol.

The users can provide the examination of various secure directing conventions of specially appointed systemutilizing table 1 at last. In table 1 demonstrates guard beside various kind of assault. Correlation demonstrates which convention is improved in various sorts of assaults.

8. Conclusions

In the current article, a brief note and some review on the various protocols available and are being used by various set of users in various set of networks like both wireless networks and ad hoc networks. Several important aspects for providing security in these sorts of protocols and theses sort of networks were discussed in brief. Various points and problems to be observed and to be discussed issues for providing security n these sorts of networkswere discussed briefly in the above sections in detail. Key administration, Ad-hoc steering of remote Ad-hoc arranges were talked about. Adhoc organizing is as yet a crude region of study can be consideringby means of the issues that survive in these systems and the rising arrangements. The input administration conventions are still exceptionally costly and not safeguard. A few conventions for directing in Ad-hoc organizes were discussed. There is a necessity to mark them additionalprotected and capable to change in accordance with the asking for essentials of these frameworks. The elasticity, straightforwardness and rapidity with which these frameworks can be customary up deduce they will expand more broad submissions. This gives the idea of Ad-hoc organizes completelyexposed for investigation to encounter these asking for submission.

References

[1] K. Singh, “A review paper on network security”, International journal of computer science and security, vol.1, no.1.Pp.52-69.
[2] A. Perrig Ran Canetti and J. D. Tygar Dawn Song, “The TESLA Broadcast Authentication Protocol”, UC Berkeley and IBM Research.
[3] A. Mahimkar and R. K. Shyamasundar, “S-MECRA A Secure Energy-Efficient Routing Protocol for Wireless Ad Hoc Networks”, IEEE 2004.
[4] A. Fourati, K. Al Agha and H. Ben Ayed, “Secure and Fair Auctions over AdHoc Networks” Int. J. Electronic Business, **(2007)**.
[5] A. Patwardhan, J. Parker, M. Iorga and A. Joshi, “Tom Karygiannis, Secure Routing and Intrusion Detection in Ad Hoc Networks”, 3rd International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, Hawaii.
[6] B. Wua, J. Wua, E. B. Fernandeza, M. Ilyasa and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks”, Journal of Network and Computer Applications, vol. 30, (2007), pp. 937–954.
[7] G.D. Bissias, M. Liberatore, D. Jensen and B.N. Levine, “Privacy vulnerabilities in encrypted HTTP streams”, In Proc. Privacy Enhancing Technologies Workshop (PET 2005).

[8] C. E. Perkins, E. M. Royer and S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV)Routing", IETF Mobile Ad Hoc Networks Working Group, Internet Draft, work in progress, vol. 17, **(2003)**.
[9] F. Hu and N. K. Sharma, "Security Considerations in Ad Hoc Networks", to be appeared in AdHon Network, **(2004)**.
[10] F. Anjum, A. K. Ghosh, N. Golmie, Paulkolodzy, Radhapoovendran, Rajeevshorey, D. Lee and J-Sac, "Security in Wireless Ad hoc Networks", ieee journal on selected areas in communications, vol. 24, no. 2, **(2006)**.
[11] H.-A. Wen, C.-L. Lin and T. Hwang, "Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients", Computers and Security, vol. 25, **(2006)**, pp. 106-113.
[12] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, "Self-securing Ad Hoc Wireless Networks", 7th IEEE Symp. on Comp. and Communications (ISCC), Taormina, **(2002)**.
[13] H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, **(2002)**
[14] H. Li, Z. Chen and X. Qin, "Secure Routing in Wired Networks and Wireless AdHoc Networks", IEEE, **(2004)**.
[15] H. Li and M. Singha, "Trust Management in Distributed Systems", IEEE Computer Society, **(2007)**.
[16] I. Aad, J.-P. Hubaux and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks", Proc. MobiCom, **(2004)**.
[17] J. Nam, S. Cho, S. Kim and D. Won, "Simple and Efficient Group Key Agreement Based on Factoring", Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '04) , **(2004)**, pp. 645-654.
[18] J. Parker, J. L. Under coffer, J. Pinkston and A. Joshi, "On Intrusion Detection in Mobile Ad Hoc Networks", In 23rd IEEE International Performance Computing and Communications Conference Workshop on Information Assurance. IEEE, **(2004)**.
[19] L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks",http://secowinet.epfl.ch/, **(2006)**.
[20] M. Bechler, H.-J. Hof, D. Kraft, F. Pählke and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks", IEEE INFOCOM, **(2004)**.
[21] M. Just_ Evangelos and K. Tao Wan, "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks", Internet draft: draft-ietfitrace-03.txt, **(2003)**.
[22] M. Al-Shurman, S.-M. Yoo and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE'04, Huntsville, AL, USA, April 2-3, **(2004)**.
[23] M. Bohio, A. Miri and E.cient, "Identity-based security schemes for ad hoc network routing protocols", Ad Hoc Networks, vol. 2, **(2004)**, pp. 309–317.
[24] N. Komninos, D. Vergados and C. Douligeris, "Layered security design for mobile ad hoc networks", journal computers & security, vol. 25, **(2006)**, pp. 121 – 130.
[25] N. Okabe, S. Sakane, K. Miyazawa and K. Kamada, "Extending a Secure Autonomous Bootstrap Mechanism to Multicast Security", 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07).
[26] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, **(2003)**, pp.27–31.
[27] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile adhoc networks, Ad Hoc Networks", IEEE, **(2003)**, pp. 193–209.
[28] R. Hinden and S. Deering. RFC 3513, "Internet Protocol Version 6 (IPv6) Addressing Architecture", **(2003)**.
[29] R. Mahajan, M. Rodrig, D. Wetherall and J. Zahorjan, "Sustaining Cooperation in Multi-Hop Wireless Networks", Proc. Second Symp. Networked Systems Design and Implementation, **(2005)**.
[30] R. Shiva Kumaran, R. Shankar Yadav and K. Singh, "Multihop wireless LAN", HIT haldia, **(2007)**.
[31] S. Holeman, G. Manimaran, J. Davis and A. Chakrabarti, "Differentially secure multicasting and its implementation methods", Computers & Security, vol.21, no 8, **(2002)**, pp736-749.
[32] S.M. Bellovin, M. Leech and T. Taylor, "ICMP Trace back Messages", Internet draft: draftietfitrace03.txt, **(2003)**.
[33] S. Yi, P. Naldurg and R. Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", IEEE, **(2003)**.
[34] S. Capkun and J.-P. Hubaux, "Building Secure Routing out of an Incomplete Setof Security Associations", WiSE'03, September 19, San Diego, California, USA, **(2003)**.
[35] W. Stallings, "Wireless Communications and Networks", 2nd Ed., Prentice Hall, **(2005)**.
[36] T. Aura, "Internet Draft: Cryptographically Generated Addresses (CGA)", http://www.ietf.org/proceedings/ 04mar/I-D/draftietf- send-cga-05.txt, **(2004)**.
[37] T. S. Messerges, ohnasCukier, T. A.M. Kevenaar, L. Puhl, R. truik and E. Callaway, "A Security Design for a General Purpose, Self-Organizing, Multihop Ad HocWireless Network", 1st ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax,Virginia, **(2003)**.

Authors

N. Thirupathi Rao, he received Ph.D. from Andhra University, Visakhapatnam, India. Currently, Dr. Rao is associated with Vignan's Institute of Information Technology, Visakhapatnam-530049, India as Assistant Head of Computer Science and Engineering. His research areas include Communication Networks, Mathematical Modeling, Image Processing, Pattern recognition, Evolutionary Computing and Security. He published 55+ research papers in various reputed International Journals and Conferences. He is the member of IE Kolkata, ACM, ISPS, CSI.

Debnath Bhattacharyya, he received Ph.D. (Tech., CSE) from University of Calcutta, Kolkata, India. Currently, Dr. Bhattacharyya is associated with Vignan's Institute of Information Technology, Visakhapatnam-530049, India as Head of Computer Science and Engineering and Dean R&D of the Institute since the year 2015. His research areas include Image Processing, Pattern recognition, Bio-Informatics, Computational Biology, Evolutionary Computing and Security. He published 200+ research papers in various reputed International Journals and Conferences. He published 6 text books for Computer Science as well. He is the member of IEEE, ACM, ACM SIGKDD, IAENG, and IACSIT.

Tai-hoon Kim, he received B.E., and M.E., degrees from Sungkyunkwan University in Korea and Ph.D. degrees from University of Bristol in UK and University of Tasmania in Australia. Now he is working for Department of Convergence Security, Sungshin W. University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments. He published 400+ research papers in various reputed International Journals and Conferences. He published 10 text books for Computer Science as well. He is the member of IEEE, ACM, *etc*.