Journal of Theoretical and Applied Information Technology
10th February 2014. Vol. 60 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY ON TRANSACTIONS BASED SECURE ROUTING IN WIRELESS NETWORKS

[1]KOUSALYA G, [2]KUMAR R

[1] Professor, Department of Computer Science and Engineering, Coimbatore Institute of Technology

[2]Assistant Professor (Senior Grade), Department of Information Technology,

Sri Ramakrishna Institute of Technology.

E-mail: [1]kousir@gmail.com, [2]rkeskumar@gmail.com

ABSTRACT

A number of transaction protocols have been proposed in recent years for possible use of Wireless Networks in various application areas such as agriculture, medical, etc. In this paper we have presented wide-ranging review of these protocols with a particular focus on their transactions model. Further we have presented a comparison of some of the existing transactions based secured routing protocols of Wireless Networks. The base criteria for comparison is routing methodologies and the information used to make routing decisions. All the protocols have to meet different security attacks, with respect to which the analyses of secure versions of proposed protocols are discussed.

Keywords: *AODV, SEAD, MANET.*

1. INTRODUCTION

This Wireless networking can be proved to be very useful in public places like libraries, guest houses, hotels, cafeterias, and schools. These are all the places, where one can find wireless access to the Internet. From a monetary approach, this is favorable to both the provider and the client. The provider would recommend the service for a charge, perhaps on a pay for each use system, and the client would be able to take advantage of this service in a convenient setting, away from the workplace or dwelling. A drawback of the wireless Internet is that, the QoS (Quality of Service) is not guaranteed and if there is any obstruction with the link, then the correlation may be dropped.

There are two discrete approaches for enabling the wireless communication among mobile hosts. The foremost approach is, by using a fixed network infrastructure, which provides wireless access points. In this network, a mobile host can communicate with the network through an access point surrounded by its communication radius. Once it goes out of range of one access point, then it is connected with a new access point within its range and then starts communicating through it. Cellular network infrastructure may be an illustration of this type of network. A major crisis of this approach is handoff, which tries to handle the situation while a connection should be smoothly handed over from one access point to the other, without any conspicuous delay or packet loss.

Wireless networks offer rapid, untethered access to information and computing, thus eliminating the barriers of distance, time, and location for the purpose of many applications that ranges from mutual, circulated mobile computing to disaster recovery (such as fire, flood, earthquake), law enforcement (crowd control, search and rescue) and martial communications (command, control, surveillance, and exploration). An ad hoc network is a compilation of wireless mobile hosts that forms a temporary network without the aid of any traditional infrastructure or federal administration. In ad hoc wireless networks, each device has the role of router and it actively participates in data forwarding. Direct communication can be performed between two nodes, if the objective is within the sender's transmission range, or in the course of intermediate nodes acting as routers (multi-hop transmission) if the objective is outside the sender's transmission range.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. LITERATURE REVIEW

Sumi Helal, et al [1], in the direction of consent, a unified incorporation between wireless LANs and Wireless WANs, they established a full stack alteration model and simple subnet architecture that place over Mobile-IP on cellular-type wireless LANs. The idea was to use Mobile IP as an integrative layer, a highest different LAN/WAN networks. Despite the fact that Mobile-IP was broadly used in wireless WANs, it was not recognized how glowingly it performs under a wireless LAN environment, counter to native MAC-level handoff. By a complete test using 802.11 W-LAN, they found that lower than practical standards of handoff frequencies, the demonstration of Mobile IP based W-LAN handoff was nearly matching to the performance of W-LAN handoff. Additional performance readings show the appropriateness of Mobile-IP as an integrative layer in this architecture.

They proposed an architecture that aims at integrating wireless LANs and Wireless WANs, and showed the title role of the Mobile-IP protocol as an integrative layer in that architecture. They also presented a simple subnet architecture that allows them to cover Mobile-IP on Wireless LANs. They found that, under practical values of handoff frequencies, the presentation of Mobile IP created W-LAN handoff is almost identical to the performance of W-LAN handoff.

Kimaya Sanzgiri, et al [2], proposed a solution to first, the managed-open scenario, where no network infrastructure is pre-deployed, however a small quantity of preceding security coordination is expected. Their protocol, Analyzing security of Authenticated Routing (ARAN), is based on certificates and successfully defeats all identified attacks. Existing ad hoc routing protocols are subjected to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of-service attacks. They introduced the notion of a tunneling attack, in which cooperating malicious nodes can encapsulate messages between them to subvert routing metrics. Protocol of ARAN, provides a solution for securing routing in the managed-open environment. ARAN provides authentication and non-repudiation services using pre-determined cryptographic certificates that guarantees end-to-end authentication. ARAN is a simple protocol that does not require significant additional work from nodes within the group. The results show that ARAN is as efficient as AODV in discovering and preserving routes, at the cost of using greater routing packets which results in a higher overall routing load, and at the cost of greater latency in route discovery because of the cryptographic computation that must occur.

Yih-Chun Hu, et al [3], proposed design and evaluation of SEAD, a new secure ad hoc network routing protocol using distance vector routing. Many previous routing protocols for ad hoc networks have been based on distance vector methods, but they have commonly assumed a reliable environment. Instead, in designing SEAD, they carefully fit low-cost cryptographic primitives to each part of the protocol functionality to create an efficient, practical protocol that is robust against multiple uncoordinated.

The attackers those who are generating incorrect routing state in any other node even in spite of active attackers or compromised nodes in the network. Organized with existing methods for securing the physical layer and MAC layer within the network protocol stack, the SEAD protocol provides a foundation for the secure operation of an ad hoc network. They base the design of SEAD in part on the DSDV ad hoc network routing protocol, and in particular, on the DSDV-SQ version of the protocol, which has been exposed to outperform other DSDV versions in preceding detailed ad hoc network simulations. For security, they use efficient one-way hash functions and do not use asymmetric cryptographic primitives. Consequently, SEAD is efficient and can be used in networks of computation- and bandwidth-constrained nodes. SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio, even though it does create more overhead in the network, both due to an increased number of routing advertisements it sends, and due to the increase in size of each advertisement due to the addition of the hash value on each entry for authentication.

Ozan K. Tonguz, et al [4], proposed the system remains the integrated cellular and ad hoc relay (iCAR) system, wherever an overlay ad hoc network is employed to use the resources efficiently by dynamically balancing the load of the *hot spots* in the cellular network, and to offer quality-of-service to subscribers, no trouble where they are placed and when the demand is completed. It is expected that this overlay network functions in the 2.4-GHz Industrial, Scientific, and Medical (ISM)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

band and the number of available ISM-band relay channels used for load balancing will be limited due to other users' interference at a given point in time. The impact of ISM-band interference on the performance of iCAR systems, which was a characteristic hybrid wireless network and it was shown that dynamic load balancing and sharing capabilities of iCAR systems were strictly dependent on the availability of the ISM-band relay channels. In adding to measuring the impact of the number of available relay channels on the performance of iCAR systems, a simple channel mission order to reduce the show dreadful conditions due to other users' interference was also provided. The result shows interference avoidance technique can improve the realistic performance of iCAR-like hybrid wireless networks.

Dynamic load balancing and sharing performance of integrated wireless networks was intentional, through a representative system called iCAR system, which functions at the cellular and the ISM-band. It happened showing that the realistic performance of iCAR systems will depend on the number of available ISM-band channels at a given point in time. The minimum number of relay channels essential for dynamic load balancing and load sharing was also counted. These results suggest that other user's interference in the unlicensed ISM-band may possibly affect the dynamic load balancing and/or sharing capabilities of this wireless system. From the proposed example, it exists shown that the number of available ISM-band relay channels will indeed be limited due to other technologies' interference and, hence, the performance of iCAR will be strictly determined by the availability of relay channels. The solution to this problem may be to design iCAR systems with interference rejection or avoidance capability. Finally, they were also providing a simple interference avoidance solution employing a channel assignment scheme based on *C/I* measurements to improve the performance of iCAR. The proposed simple solution can improve the performance by 12%–23% when the interferers were uniformly distributed and by 60%–90% when they have a normal distribution.

Xiaoqi Li, et al [5], proposed a novel secure routing protocol for MANETs. This protocol TAODV (Trusted AODV) extends the widely used AODV (Ad hoc On demand Distance Vector) routing protocol and services the idea of a trust model to defend routing behaviors in the network layer of MANETs. In the TAODV, trust among nodes is characterized by opinion, which is an item derived from subjective logic. The ideas are dynamic and updated frequently as their protocol specification: If one node performs normal communications, its estimation from other nodes' points of view can be increased; then, if one node performs some malicious behaviors, it will be ultimately shorn of by the whole network. A trust approval mechanism is also designed to exchange trust information between nodes. The outstanding feature of TAODV is that using trust interactions among nodes, there is no need for a node to request and verify certificates all the time. This importantly reduces the computation overheads. In the meantime, with neighbors' trust approvals, a node can make objective judgment about another node's trustworthiness to maintain the whole system at a certain security level.

Jianhong Xia, et al [6], overflows attacks that exploit routing differences in the Internet. In exact, they focused on routing anomalies presented by persistent forwarding loops. These loops may share one or more links with progressing routes to accessible addresses. An attacker can exploit persistent forwarding loops to overload the shared links to disrupt the Internet connectivity to those reachable addresses. To understand the extent of this vulnerability, they performed general measurements to analytically study persistent forwarding loops and the number of network addresses that can be affected. They found that persistent forwarding loops do exist in the current Internet. About 0:2% of routable addresses experience persistent forwarding loops and 0:21% of routable addresses can be attacked by exploiting persistent forwarding loops. In addition, 85:16% of the persistent forwarding loops appear within destination domains and they can be observed from various locations, which make it possible to launch attacks from many vantage points. They also found that most persistent forwarding loops were just two hops long, which allows an attacker to amplify traffic to persistent forwarding loops significantly. The best of result the persistent forwarding loops to launch DDoS attacks and also they investigate the vulnerability on flooding attacks by exploiting persistent forwarding loops. In that, the highlight such vulnerability can be broken from various locations, and can strictly affect the Internet connectivity to important number of network addresses. These outcomes suggest that this vulnerability could be a critical threat to the Internet security.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Yih-Chun Hu, et al [7], presented the design and estimation of Ariadne, a new secure ad hoc network routing protocol. Ariadne delivers security against one compromised node and arbitrary active attackers, and trusts only on efficient symmetric cryptographic operations. Ariadne works on-demand, dynamically discovering routes between nodes only as required; the design is based on the simple operation of the DSR protocol. Rather than kindly applying cryptography to an existing protocol to achieve security, however, they carefully re-designed each protocol message and its processing. The security mechanisms they designed are highly efficient and general, so that they should be appropriate to securing a wide variety of routing protocols. Because, it does not secure the optimizations of DSR in Ariadne, the resulting protocol is less efficient than the highly optimized version of DSR that runs in a trusted environment.

The compared Ariadne to a version of DSR in which they disabled all protocol optimizations not present in Ariadne. Ariadne actually performs *better* on some metrics (e.g., 41.7% lower packet overhead) than for unoptimized DSR, and about the same on all other metrics, even though Ariadne must bear the added costs for security not present in unoptimized DSR. They found that source-routing facilitates securing ad hoc network routing protocols. Source routing empowers the sender to avoid potentially malicious nodes, and enables the sender to validate every node in a ROUTE REPLY. Such fine-grained path control is absent in most distance vector routing protocols, which makes such protocols more challenging to fully secure.

Stephan Eichler, et al [8], proposed a new secure routing protocol for mobile ad hoc networks (MANETs) based on Ad-hoc On-Demand Distance Vector (AODV) titled AODV-SEC. This security method is using certificates and a public key infrastructure as trust anchor. In addition they were presented the need for a new certificate type for secure routing in MANETs called *mCert*. The simulation results not only prove the functionality and performance of the protocol, moreover, they can be used to point out general challenges for the design and use of secure routing protocols in MANETs. In their estimation the results point out the current difficulties of secure routing protocol design. An important concern for the usability of a secure routing protocol is the presentation of the implemented cryptographic mechanisms. This performance has not yet been investigated previously. Hence, we compared the two cryptographic libraries *libcrypto* and *Crypto++*. They results proved that the performance of a crypto library can be good adequate to implement a secure routing protocol or MANETs. Observably, the presentation always depends on the hardware performance. However, even a rather slow system is accomplished of calculating all necessary security functions in about 60ms. This delay is small enough to be acceptable for a MANET routing protocol. Therefore, cryptographic functions and their calculation delay are not a problem for the implementation of a secure routing protocol. Closely related to the cryptographic mechanisms are the distribution and the handling of certificates. In their approach the certificates are distributed within the request and reply packets of the protocol. This approach is not essentially the most active, however, no other certificate exchange protocol is needed using this approach. Moreover, in large networks it is not achievable to distribute all certificates in the network. During their simulations, the encountered a performance concern related to this certificate handling mechanism. The size of regular X.509 certificates is too large to fit all necessary data information into a single request. Therefore the MAC-layer jumps to fragment packets, resulting in twice the number of packets on the channel, accumulative the possibility of collisions.

Babu, et al [9], proposed a novel Transaction Based Authentication Scheme (TBAS) for mobile communication using cognitive agents. This approach intensifies the procedure of authentication by deploying authentication scheme based on the transaction sensitivity and client's transaction time behaviors. The TBAS provides an effective authentication solution by relieving the conventional authentication systems from being dependent on only the strength of authentication identifiers. In addition the transaction time behavior analysis by cognitive agents provides rational approach towards establishing the legitimacy or illegitimacy of the mobile client. This method has been simulated with different applications over in-house established wired and wireless networks. The Agent Factory framework is utilized for cognitive agents generation and communication.

Pallapa Venkataram, et al [10], proposed a transaction-based authentication scheme for PMM applications using cognitive agents. The planned method dynamically deploys authentication

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

challenges based on mobile transaction sensitivity and users transaction time behaviors. They provide the performance analysis of the authentication scheme in terms of authentication delay and cost. The performance analysis displays that, there is a substantial reduction in security cost compared to regular session based authentication schemes. By merging transaction based authentication with behavior analysis authentication attacks can be effectively identified.

In PMM-TBAS, the authentication process is constant throughout the session; it is not dependent only on the first time successful verification of authentication identifiers. The authentication process is not fixed; it keeps the changing sensitivity levels of transactions and beliefs deviation in order to propose the authentication challenges whenever required during the session. The scheme would be watchful from the beginning for a mischievous user whose track history is very bad. The scheme is pro-active in terms of sensing suspiciousness and blocking the critical transactions from execution, so that the unexpected behaviors of genuine users are handled with minimum interruptions.

Baruch Awerbuch, et al.[11], ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or conspiring nodes. The protocol uses an adaptive probing technique that detects a malicious link after log *n* faults have occurred, where *n* is the distance of the path. Challenging links are avoided by using a route discovery mechanism that relies on a new metric that captures adversarial behavior. The protocol never partitions the network and bounds the amount of damage caused by attackers.

Zhen Cao, et al [12], proposed a *Feedback based Secure Routing protocol* (FBSR). Feedback from the neighboring nodes serves as the dynamic information of the existing network, with which sensor nodes make advancing decisions in a secure and energy aware manner. Feedback message is included in the MAC layer acknowledgement frame to avoid network congestion, and it is authenticated with the proposed Keyed One Way Hash Chain (Keyed-OWHC) to avoid feedback fabrication. Furthermore, we enhance FBSR's resilience to node compromise by statistic efforts accomplished by the base station. FBSR is proposed for adaptable and defendable routing in wireless sensor networks. They present the Keyed One Way Hash Chain (Keyed-OWHC) to authenticate feedback from neighbors, and use the statistic detection on base station to discover potentially compromised nodes, hence making FBSR resilient to existing routing attacks.

Pallapa Venkataram, et al., 2009, proposed a novel Transaction Based Authentication Scheme (TBAS) for mobile communication using cognitive agents. This approach provides range of authentication based on mobile transaction compassion, and user's performances. The TBAS uses mobile agents to collect user behaviors, and static agents for sensing transaction sensitivity, user history investigation, and for indicating suitable authentication actions. This method has been simulated using the agent factory outline for cognitive agents' generation and their message. The performance analysis and the simulation of the proposed system shows that there is a considerable reduction in the security cost compared to regular session based authentication schemes. By merging transaction based authentication with behavior analysis the authentication attacks can be efficiently identified.

Bhalaji N, et al [13], proposed a new approach based on relationship among the nodes which makes them to cooperate in an Adhoc environment. The trust component is used to calculate the trust values of each node in the network. The designed trust values are being used by the association estimator to determine the relationship status of nodes. The proposed improved protocol was compared with the standard DSR protocol and the scheme of Trust Enhanced DSR protocol increases the level of security routing and also encourages the nodes to cooperate in the adhoc structure. It identifies the malicious nodes and isolates them from the active data forwarding and routing.

Sadek, et al [14], proposed a Real-time Host Intrusion Detection for Ad hoc Networks (REHIDAN) technique to recognize the selfish nodes in the ad hoc network. An AODV-based REHIDAN technique is obtainable to take the suitable countermeasures to minimize the efficiency of the attack and maintain the network performance within the accepted limits. The results show that the proposed REHIDAN technique reduces the end-to-end delay and the routing overhead ratio.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Qabajeh, et al [15], proposed a new model of routing protocol called ARANz, which is an addition of the original authenticated routing for ad-hoc networks (ARAN). ARAN objectives to increase security complete robustness and solve the single point of failure and attack problems by introducing multiple local certificate authority servers.

Ming Yu, et al [16], proposed trustworthiness-based quality of service (TQOS) routing, which contains secure route discovery, protected route setup, and trustworthiness-based QoS routing metrics. The routing control communications are secured by using both public and shared keys, which can be produced on-demand and preserved dynamically. The message swapping mechanism also provides a way to detect attacks against routing protocols, typically the most difficult internal attacks. The routing metrics are found by combing the requirements on the trustworthiness of the nodes in the network and the QoS of the links along a route.

Hua-Yi Lin, et al [17], presents a hypercube routing algorithm with secure data transmissions, which offers rapid, efficient and fault-tolerant routing mechanisms using elliptic curve Diffie-Hellman (ECDH) scheme to achieve key agreements and secure data transmissions. Meanwhile, ECDH uses a small key length 160-bit to achieve well-suited security levels on 1024-bit Diffee-Hellman (DH), therefore sensor nodes only essential few CPU, memory and bandwidth to complete security operations. Subsequently, the proposed routing algorithm with secure data transmissions can perform very fast and professionally, and are highly suited for wireless sensor networks (WSNs) with limited resources.

Jyu-Wei Wang, et al [18], proposed a secure destination-sequenced distance-vector routing protocol (SDSDV) for ad hoc mobile wireless networks and the protocol is based on the regular DSDV protocol. Inside SDSDV, each node maintains two one-way hash chains about each node in the network. Two extra fields, which called AL (alteration) field and AC (accumulation) field, are additional to each entry of the update packets to carry the hash values. With appropriate use of the elements of the hash chains, the sequence number and metric values on a route can be threatened from being arbitrarily tampered.

Yao Lan, et al [19], proposed a multipath secure routing protocol for flat network--MDMP. Symmetric encryption and asymmetric encryption are exploited to encrypt and validate data in the network. Also, malicious nodes will be detected out and isolates. The results show that MDMP provides effective immunity to a variety of attacks in WSN and better network performance.

Gopalakrishnan Nair, et al [20], proposed model defines an application of Cognitive Network to improve the network performance by applying a Hidden Markov Model (HMM) algorithm for learning and predicting the performance of adjacent routers continuously while a routing demand is introduced. The cognition division/area of every router can increase knowledge about the quality of forward network. The evidence of the current network conditions is shared between routers by the "Forward Channel Performance Index (FCPI)". This enables complete cognition of surroundings and efficient delivery of messages in various paradigms of performance.

The implementation of an efficient Cognitive Network, which works with learning and prediction capability of its surroundings using HMM. The learning, combined with reasoning works well in the Cognitive Domain along with the routing functions of Routing Domain in a Cognitive to look forward to the next hop point layers successfully for reconfiguration of the path offering much better delivery assurance compared to blind routing as prevalent in conventional devices. The planning unit in the cognitive domain advises the routers administrator about the future level of QoS and the service types expected from other routers. The major advantage in this approach is the extremely low level of cognitive packet transport in the network enabling almost full capacity utilization of channels while having a high degree of cognition about the current network state at each node.

Sathish Babu, et al [21], proposed a new trust model based on cognitive reasoning, which connections the notion of trust with all the associate nodes of MANETs using a novel Behaviors-Observations- Beliefs (BOB) model. These trust standards are used for discovery and avoidance of malicious and fraudulent nodes while routing the data. The planned trust model works with the DTM-DSR protocol, which involves totaling of direct trust among any two nodes using cognitive

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

knowledge. They had taken care of trust failing over time, rewards, and penalties while computing the trustworthiness of a node and also route. The results of experiments displays combination of cognitive reasoning for computation of trust in routing efficiently detects intrusions in MANET environment, and generates more consistent routes for secured routing of data.

Mayuri Gund, et al [22], proposed a multi-agent based mobile health monitoring system which is the grouping of a wireless medical sensor unit with data mining methods. Mobile Health Care is the application of mobile computing technologies for refining communication amongst patients, physicians and other health care workers. They explained separate Association rule exploration into two data groups: 1) Real time sensory data collected from patient's body 2) Historical data collected in past. This system collects the diagnosis patterns, then classifies them into normal and emergency terms and declares emergency by comparing the two data groups as mentioned earlier. Thus suggests methods to analyze and model patterns of patient's normal and emergency status.

The planned a ubiquitous healthcare system by demonstrating real-time diagnosis and treatment services provided by a hospital system, based on collected medical and peripheral data. The proposed system offers an interconnection of patients and a hospital in a ubiquitous computing environment. In multi-agent system, agents are involved in functions, such as using sensors to accumulate medical and peripheral data in real-time, storage the collected data in the IMS, determining whether a patient is in a critical condition, transferring to the hospital system data about the patient that has been determined to be critical, and finally delivering the doctor's diagnoses and prescriptions to the patient. However, determination of the patient's condition in medical terms based on the collected data requires further investigation. Once the technology is refined, medical costs for correcting chronic medical conditions will be reduced .Our goals will be fulfilled if the E-Healthcare System can help a single individual by monitoring his or her health and cautions him to take necessary actions against any upcoming serious diseases.

Tao Gong, et al [23], proposed an ad hoc on-demand position-based private routing protocol (AO2P), but the AO2P is vulnerable to some collaborative attacks, such as blackhole & wormhole attacks. Once any compromised node is included in a route, it can conduct different attacks, which are very difficult to identify because of the pseudo identifiers in the AO2P. In order to immunize the mobile ad hoc networks against the collaborative attacks and enhance the security of the private routing protocol, a novel secure and immune private routing protocol is proposed and called as NSIPRP. The NSIPRP is based on the native immunization of mobile nodes and the immune reconfiguration of the mobile ad hoc networks, and can be used to protect private information against the collaborative attacks. The results show that, while the NSIPRP immunizes the mobile ad hoc networks against the collaborative attacks and preserves communication privacy in the mobile ad hoc networks, its routing performance is similar with other position-based routing algorithms such as the AO2P.

Patil, et al [24] proposed a location and energy efficient routing scheme using identity bases cryptography. They review the classical selective forwarding attack on WSN and see how an identity-based cryptographic scheme using a cross-layer design approach is helpful in circumventing such an attack. In addition, they show that an identity-based cryptographic approach to routing in WSN is more pragmatic then the traditional public key infrastructure (PKI) based schemes. The identity-based cryptography can play a vital role in defending against many complex cross-layer attacks on WSN routing protocol. As an example, they show how location and energy aware identity-based cryptographic routing can prevent a selective forwarding attack. Moreover, secure cross-layer approach allows intermediate routing nodes to make protected, intelligent routing decisions to prevent route-suppression attacks.

3. CONCLUSION

In this paper we have presented the best known protocols for transactions based secure the routing function in wireless networks and provided comparisons between them. Apart from that, there are still many challenges facing secure routing in wireless networks. The analysis of the different proposals has demonstrated that the inherent characteristics of wireless networks, such as lack of infrastructure and rapidly topologies, introduce added difficulties to the already complicated

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

problem of secure routing. This is why Wireless Networks are becoming more and prevalent in the world. The evaluation we have presented between the routing protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing security solutions. Finally, we consider that more work is still required to justify the exact definition for secure routing which will allow researchers to formally prove whether a proposed protocol satisfies all the security issues concerning wireless networks.

REFERENCES:

[1] Helal S 2000, 'An Architecture for Wireless LAN/WAN Integration', *Wireless Communications and Networking Conference*, vol.3, pp. 1035 – 1041.

[2] Kimaya Sanzgiri, Bridget Dahill 2002, 'A Secure Routing Protocol for Ad Hoc Networks', *10th IEEE International Conference on Network Protocols.*

[3] Yih-Chun Hu, David B. Johnson, Adrian Perrig 2003, 'SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks', *Journal of Ad Hoc Networks, Elsevier*, 2003, pp. 175-192.

[4] Hongyi Wu, Chunming Qiao, Swades De, Ozan Tonguz 2004, 'Integrated Cellular and *Ad Hoc* Relaying Systems: iCAR', *IEEE Journal on Selected Areas in Communications*, Vol.19, No.10, pp.2105-2115.

[5] Xiaoqi Li, Michael R Lyu, Jiangchuan Liu 2004, 'A Trust Model Based Routing Protocol for secure Ad Hoc Networks', *IEEE Aerospace Conference*, vol. 2, pp. 1286-1295.

[6] Jianhong Xia, Lixin Gao, Teng Fei 2005, 'Flooding Attacks by Exploiting Persistent Forwarding Loops', *IMC '05 Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, pp. 36.

[7] Yih-Chun Hu , Adrian Perrig 2005, 'Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks', *Journal of Wireless Networks, Springer*, vol. 11, pp. 21-38.

[8] Stephan Eichler, Christian Roman 2006, 'Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC', *Mobile Adhoc and Sensor Systems (MASS), IEEE International Conference*, pp. 481-484.

[9] Babu B.S, Venkataram P 2007, 'Transaction Based Authentication Scheme for Mobile Communication: A Cognitive Agent Based Approach', *IEEE International Parallel and Distributed Processing Symposium (IPDPS 2007)*, pp.1-8.

[10] Sathish Babu B, Pallapa Venkataram 2008, 'Performance Analysis of an Authentication Scheme for Personalized Mobile Multimedia applications: A Cognitive Agents based Approach', *International Journal of Security and its Applications*, vol.2, no.4, pp. 117 – 140.

[11] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens 2008, 'ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks', *ACM Transactions on Information and System Security (TISSEC)*, vol.10.

[12] Zhen Cao, Jianbin Hu, Zhong Chen, Maoxing Xu, Xia Zhou 2008, 'FBSR: Feedback based Secure Routing Protocol for Wireless Sensor Networks', *International Journal of Pervasive Computing and Communications*, vol.4, pp.61-76.

[13] N Bhalaji, A R Sivaramkrishnan, Sinchan Banerjee, V Sundar, A Shanmugam 2009, 'Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks', *World Academy of Science, Engineering and Technology*.

[14] IBRAHIM M.M, SADEK N, EL-BANNA M 2009, 'PREVENTION OF DROPPING ROUTING TRAFFIC ATTACK IN WIRELESS AD-HOC AODV-BASED NETWORKS USING REAL-TIME HOST INTRUSION DETECTION', *RADIO SCIENCE CONFERENCE*, PP.1-9.

[15] Qabajeh L.K, Kiah L.M, Qabajeh M.M 2009, 'A Scalable Secure Routing Protocol for MANETs', *International Conference on Computer Technology and Development (ICCTD '09)*, vol.1, pp.143-147.

[16] Minh Yu, Leung K.K 2009, 'A Trustworthiness-based QoS routing protocol for wireless ad hoc networks', *IEEE Transaction on Wireless Communication, vol.8*, pp.1888-1898.

[17] Hua-Yi Lin 2009, 'Hypercube Routing Protocol with Secure Data Transmission Mechanisms in Sensor Networks Using Elliptic Curve Diffie-Hellman Key Agreements', *IEEE International Conference on New Trends in Information and Service Science (NISS '09)*, pp. 1303-1308.

[18] Jyu-Wei Wang, Hsing-Chung Chen, Yi-Ping Lin 2009, 'A Secure DSDV Routing Protocol

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for Ad Hoc Mobile Networks', *IEEE Fifth International Joint Conference on NC, IMS and IDC (NCM '09)*, pp.2079-2084.

[19] Yao Lan, Luo Lei, Gao Fuxiang 2009, 'A multipath secure routing protocol based on malicious node detection', *IEEE Control and Decision Conference (CCDC '09)*, pp.4323-4328.

[20] T R Gopalakrishnan Nair, M Jayalalitha, Abhijith S 2010, 'Cognitive Routing with Stretched Network Awareness through Hidden Markov Model Learning at Router Level', *Networking and Internet Architecture*, Jan 2010.

[21] Sathish Babu B, Pallapa Venkataram 2011, 'A Trust Model for Routing in MANETs: A Cognitive Agents based Approach', *WorldComp-2011*, Las Vegas, USA.

[22] Mayuri Gund, Snehal Andhalkar, Prof. Dipti Patil, Dr. V.M.Wadhai 2011, 'An Intelligent Architecture for Multi-Agent Based m-Health Care System', *International Journal of Computer Trends and Technology*, March – 2011.

[23] Tao Gong, Bharat Bhargava, Norman O Ahmed 2011, 'Novel Secure and Immune Private Routing Protocol in Mobile Ad Hoc Networks', *IEEE Transaction on Mobile Computing*.

[24] H. Patil, J Camp, S Szygenda 2011, 'Secure Routing in Wireless Sensor Networks using Identity-based Cryptography', *International Journal of Applied Science and Technology*, vol.1(5), pp.1-14.