International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-7, May 2020

Routing Architectures for IoT

Kamalinder Kaur, Sandeep Kang

Abstract: ***In today's technologically driven world, numerous physical activities can be digitally controlled with a single click, which has led to the emergence of the Internet of Things as an innovative prospect strengthened by MANET and WSN. The present study covers the review of various routing protocols and algorithms related to IoT in MANET and WSN. The review study covers the research published in highly authenticated platforms since 2010. The concept is further extended to cover the performance parameters, security, and privacy aspects adjoining the data packet transfer among various nodes. The review offered a critical examination of various solutions postulated by various researchers will further guide the futuristic research in the improvement of information transfer via a network. A couple of Quality of Service parameters including Throughput and Packet Delivery Ratio(PDR) were also analytically analyzed for various routing architectures supporting IoT environment.***

Keywords*: MANET, IoT, WSN, Routing Protocol.*

I. INTRODUCTION

Today internet has become an indispensable part governing even the smallest need of day-to-day life. A wireless linked interconnected network node of the internet constitutes an Ad-hoc network. A Mobile Ad-hoc Network (MANET) shown in Fig. 1. is a variant of Wireless Ad-hoc Networks that demonstrates unique self-configuring and decentralized organization [1-2]. Bellavista et al. summarized that Wireless Sensor Network (WSN) and MANET have together motivated the idea of deploying vivid internet-driven IoT applications, as summarized in Fig. 2. [3]. The nodes of the networks act as routers communicating data packets and information from source to the sink or from the sender to the receiver. MANET has offered diverse applications such as laptops, mp3 players, and cell phones, etc. that require low bandwidth [4]. It offers potential applications during rescue operations when existing infrastructures have been destroyed. MANET here aimed to design a Bluetooth network to offer communication channels [5]. However, MANETs offers energy and bandwidth controlled operation with dynamic topologies; it is still a victim of limited physical security. In this scenario, Internet-of-things is the latest innovation connecting physical things with the digital world. Since the last decade, the development of Internet-of-Things has encouraged a new paradigm to offer controlling mechanisms to manage various IoT devices with the aid of the internet.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Kamalinder Kaur*, Research Scholar, Department of CSE, Chandigarh University, Punjab, India. E-mail: kaur.kamalinder2017@gmail.com.
Dr. Sandeep Kang, Professor, Department of CSE, Chandigarh University, Punjab, India. E-mail: sandeepkang.cse@gmail.com

In this regard, Bruzgiene et al. addressed the characteristics, challenges, application, and security of MANET in IoT devices [6]. Routing is described as a process that determines the path of nodes followed by the data packets in a communication channel. Conventions and principles that govern the node selection and direction of propagation of data packets or signals constitute the routing protocol that offers greater challenges [7].

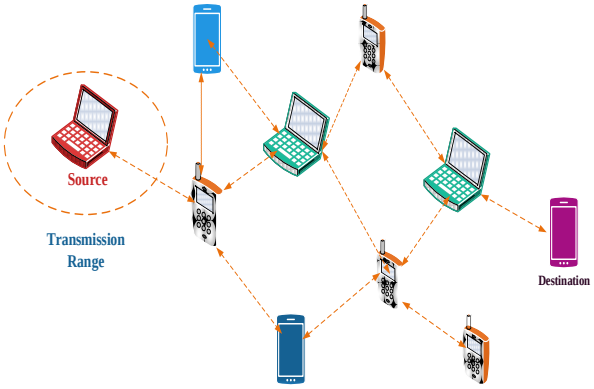

Fig. 1. Mobile Ad-hoc Network

Kaur et al. presented a survey of routing mechanisms in which routing protocols are broadly classified as proactive, a routing protocol that works on tabular architectures, reactive routing protocols that are on-demand, and the hybrid routing protocols that are the combination of proactive and reactive routing protocols [8].

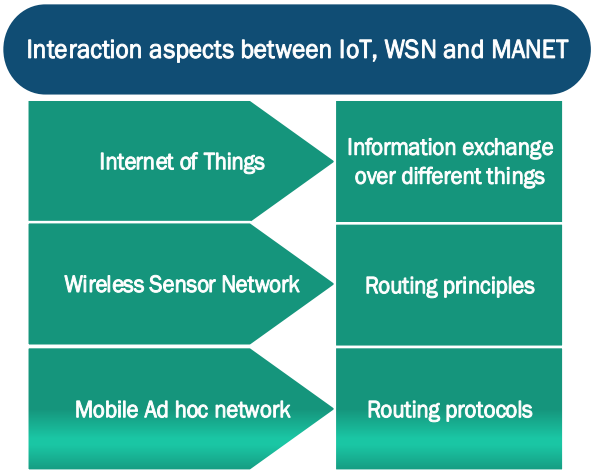

Fig. 2. Interaction among MANET, WSN, and IoT

Among these, hybrid routing protocols have largely attracted vast research community to trace the best path between source and destination with the implementation of numerous routing protocols. The goal of this paper is to offer a critical review of various existing routing protocols, their strengths, limitations, and security aspects to guide futuristic research direction.

The review paper is organized into five sections. Section 1 covers the introduction, section 2 summarizes the implemented data mining strategies, and section 3 covers the review studies whose outcomes are summarized in section 4. The paper is concluded in section 5.

II. METHODOLOGY

The study design acknowledges data mining of standard routing protocols for IoT in MANET and WSN. This involves an intensive search of technical and research articles published in various authenticated platforms, namely, PubMed, Science Direct, IEEE, Google Scholar, Scopus, and Springer. The keywords like "MANET", "Internet-of-Things", "IoT", "WSN", "Wireless Sensor Network", "Mobile Ad-hoc Network", "routing", "routing protocols", "root discovery", "security", "attacks" have been used with and without "protocol", "tools", technologies", "solution", "approaches" and "analytics". This has resulted in a large number of papers. The search results in a large amount to patents and papers. To increase the proportion of the most relevant search results filtering criteria are applied as described in the flow diagram shown in Fig. 2. The data mining is restricted to papers that are published from 2010 to date. The paper language is also restricted in order to easily understand the published research and the described routing protocols of various researcher.

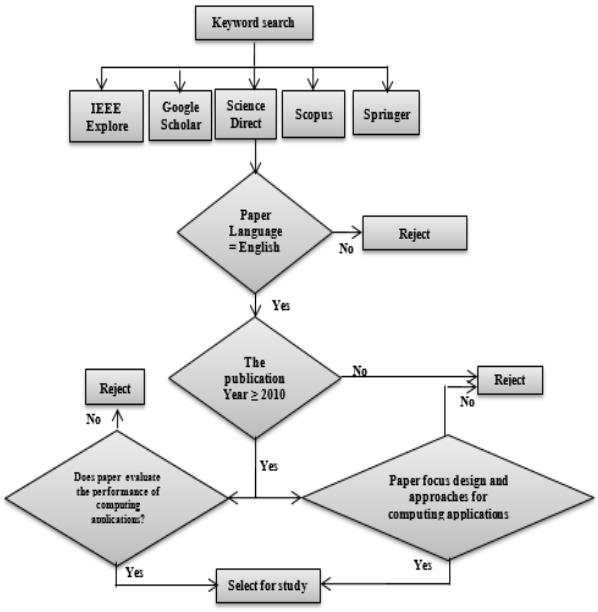

Fig. 3. Data mining framework

Initial searches have resulted in more than 600 papers that were related to MANET, WSN, and IoT applications. Further, the short-listing is done on the basis of filtering on the basis of published years that decreased the mining results to 250. Further, more inclusion and exclusion criteria were implemented based on language, routing design, applications, and approaches, etc. that decreased the papers list to 84. Finally, out of these 84 papers, only 30 papers were selected for critically analysis and reading the research content of respective papers. Next, the constructive review is presented of the considered papers in reference to applications, routing protocols, and root discovery approaches implemented in reference to IoT in MANET and WSNs.

III. LITERATURE SURVEY

The development of a secure platform has been addressed by postulating various proactive, reactive, and hybrid routing protocols, various researchers. In this regard, **Bakshi et al.** had discussed various routing protocols and summarized that MANETs offers greater data packet mobility as compared to various wired network solutions. A critical comparative analysis of available routing protocols had also been summarized [9]. **Serhani et al. (2019)** proposed an Adaptive Q-learning protocol to address mobility issues concerning MANET and IoTs. In the process, the Q-learning approach was also used based on the Qmatrix governing dynamic and static routing and network topologies. The protocol proved to be effectively used as a network mobility mode while increasing the PDR of widely used MANET-IoT designs [10]. **El-Tager and Gadallah 2019** had proposed Socially Weighted Shortest path routing protocol that proved to be very effective in addressing the routing issues of social networks. The effectiveness of the design was evaluated against various routing protocols aimed at finding the shortest routing path [11].

A. Approaches dealing with Routing Protocols

Singla et al. (2010) evaluated various routing protocols, including AODV reactive and DSDV, as proactive MANET routing protocols based on the TCP and CBR traffic patterns. Based on the CBR traffic patterns, AODV had performed better than DSDV in terms of delay, throughput, and packet delivery ratio [12]. When the MANET attributes are supplied to vehicles, the network is termed as VANET. **Kabir et al.** (2015) found that most of the existing routing protocols designed for MANETs were not applicable to VANETs. Hence, they postulated a Pro-AODV that took the advantage of routing tables of AODV to reduce the jamming instances prevailing in VANETS. The salient feature of the design was that knowledge of routing table size was enough for the apt performance of the design [13]. **Gandhi et al. (2012)** offered the simulator-based critical comparison of AODV, DSDV, and ZRP using the Random Way-point model. They concluded that AODV to be the most viable routing protocol out of the three routing protocols [14]. **Ravi and Kashwan (2015)** presented a new energy-saving strategy addressed with Energy-Aware Span Routing Protocol (EASRP). This algorithm implements energy conservation using an adaptive energy conservation algorithm and span. Simulation analysis against EAZRP and ZRP established that the proposed EASRE outperformed by demonstrating 12.2% and 17.45% enhanced energy efficiency [15].

Rajaram and Sugesh (2011) addressed routing issues of energy conservation and discovering the shortest path with the proposed Power-Aware Ad-hoc on-demand Multiple Distance Vector (PAAOMDV). The proposed protocol worked by regularly revising the routing tables with the latest information pertaining to the node and their respective energy values.

The simulation studies showed that the proposed design outperformed the AOMDV (Ad-hoc On-demand Multipath Distance Vector) routing protocol [16]. **Vashistha (2014)** focussed his study on enhancing the effectiveness of the AOMDV routing protocol. In the process, he improved the performance of the network demonstrated by the offered quality of service by randomly changing the query length and multiple path schemes [17]. **Zhang et al. (2019)** designed QG-OLSR, which was a modified OLSR protocol based on quantum-genetics. The design offers a combination of OLSR and Q-learning approaches to optimize multi-point relay sets. The authors had demonstrated that the design proved to be minimizing energy consumption while improving the PDR and network delay. Overall, the modified protocol proved to be highly effective in numerous MANET applications [18]. The main idea behind the implementation of on-demand Ad-hoc Networks is that it focuses on discovering the necessary routes only. **Jaisankar and Saravanan** postulated a multipath route discovery scheme that demonstrated effectiveness in tracing multiple routes about single route discovery. The scheme exemplified the implementation of secondary paths to offer the least routing overhead.
Additionally, it was capable of discovering safe routes by offering multiple paths from source to destination. Simulation studies had shown that the proposed design is more effective than AODV in searching and preserve multiple routes [19]. **Vikram et al. (2011)** proposed a QoS-DSR mechanism that was aimed to improve the network delay of the DSR routing protocol along with maintaining a relatively higher packet delivery ratio of existing DSR protocol. The simulation results of Network Simulator II has demonstrated that the proposed design proved to effectively maintain the quality of service parameters of DSR while End-to-End delay was considerably reduced with QoS-DSR [20].

B. Approaches dealing with Security and Attacks

The security of the mobile network is an important aspect to offer safer communication in the prevailing unfriendly, and threatening environment. In MANET based communication networks, nodes organized themselves, and this characteristic further adds to the security challenge. The malicious attacks may attack physical, data or network layer. To address this issue, Ponguwala and Rao (2019) proposed a highly energy-efficient and secure routing protocol that they abbreviated as E2-SR. The design dealt with the rising issues of data protection, privacy, and veracity concerns in MANET-IoT. The authors have proposed hash-based authentication and proposed SDHC-EC as a secure dual-head clustering along with elliptic curve verification. Additionally, secure routing is offered by a new WC-PSO design that was actually referred to Worst Case Particle Swarm Optimization algorithm. The simulation studies had demonstrated effective results in terms of parametric values of throughput, routing overhead, PDR, and residual energy [21]. Alshehri et al. (2019) addressed the IoT network to offer a protected and highly reliable platform. The authors had proposed a trustworthy messaging system to offer secure communication among nodes. The designed system worked on the basis of hexadecimal values. The proposed system was evaluated for different security attacks, and the experimental results demonstrated the effectiveness of the design to offer a secure communication system [22]. El-Semary et al. (2019) addressed the security aspects of the black hole attack and proposed BP-AODV as a routing protocol. The design could successfully protect MANET against more effectively as compared to the SADOV protocol. The protocol demonstrated instrumental results to safeguard against black hole attacks during the forwarding process [23].

IV. SURVEY OUTCOMES

The presented review study offers a summary of the literature cited routing mechanisms and protocols dealing with mobile networks. In the scheme, discussed routing mechanisms fall under three categories, namely, proactive, reactive, and hybrid routing protocols, as summarized in Fig. 4. In the case of proactive routing mechanisms, DSDV and OLSR routing protocols were discussed that take advantage of the tabulated architecture. AODV and DSR are the on-demand routing mechanism, and their improvement strategies are discussed in reactive routing protocols. While the combination of proactive and reactive routing protocols was discussed under hybrid routing protocols.

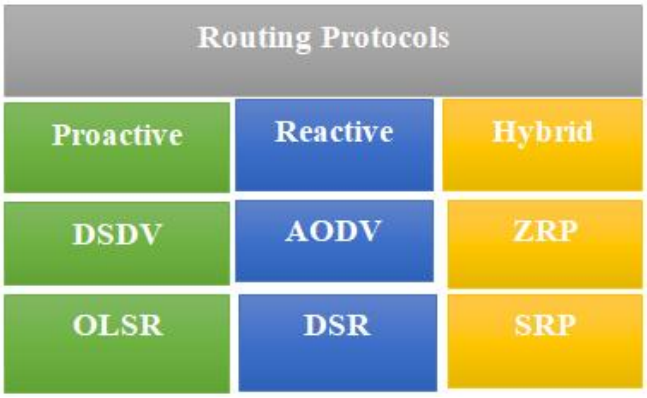

Fig. 4. Classification of Routing protocols

The revolutionizing technology has led to the refinement of various routing protocols to add security features to the traditional routing protocols. Further, important designed routing protocols studied are summarized in Table 1. along with their potential implementation and background strength. It is found that security aspects are proposed to address three different layers. Firstly, physical layer attacks cover drooping, jamming, and active interference attacks. Secondly, the data layer attack deals majorly with the dynamic aspects covering traffic analysis of the network. Thirdly, comes the malicious threats and attacks on the network layers were blackhole attack, sinkhole attack, and work hole attack have majorly attracted numerous researchers over the world.

Table-I: Literature cited enhanced Routing protocols

Application	Implementation	Reference
AQ-Routing	Based on Reinforcement Learning (RL) techniques	10
E2-SR	Secure routing for MANET-IoT	21

EASRP	An energy conservation span routing protocol	15
Extended AODV	Multipath routing scheme	19
Narrative Multipath QoS Aware Routing Protocol	Reduce routing overhead and maintain PDR	17
PAAOMDV	Address energy and path length issues	16
Pro-AODV (Proactive AODV)	AODV based jamming minimization in VANET	13
QG-OLSR	Adopts the MPR (multi-point relay) technology in OLSR (Optimal Link State Routing).	18
QoS-DSR	Minimize Network delay with high PDR	20
Scenario-based performance analysis	Random way-point model for mobility check	14

QoS evaluation is also known as Quality-of-Service evaluation is an important aspect that determines the effectiveness of the designed routing protocol. QoS is characterized by parameters that govern the scalability, stability, reliability, and security aspect of the network design. There are important performance metrics summarized in Table 2. that are usually calculated to judge the merits or limitations of the proposed solutions and designs. Among these, PDR, also known as packet delivery ratio, corresponds to the proportion of data packets that are effectively delivered to the destination. Network delay presents an end to end delay offered by the routing protocol during data transmission. Throughput magnitude is more related to the stability aspects of the router. The main idea behind referring such performance parameters here is to evaluate various proposed designs in terms of delay, throughput, and PDR values.

Table-II. Performance Analysis Parameters

Performance Parameters	Quantitative Aspect
Mobility	Reliability
Network Delay	Loop-freedom
Overhead	On-demand or proactive
Packet Delivery Ratio	Scalability
Throughput	Route stability

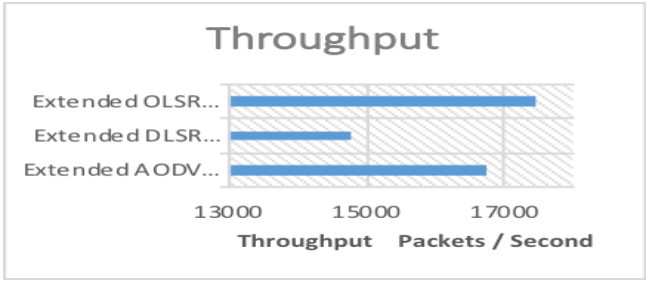

Fig. 5. Throughput

The evaluation of some of the recent research articles with QoS parameters is shown in Fig. 5 and 6 The first evaluation is made on the base of throughput, which is the total number of received packets per second and the second parameter is PDR which is the ratio of the received packets to the sent packets. It is observed that the extended OLSR protocol, which takes some of the advantages of the AODV as well performs better than both extended AODV and extended DSR, which were proposed in [19] and [20] respectively. The average throughput of the e-OLSR is noted to be more than 17000 units per second, whereas, for a similar environment, e-DSLR computes below 15000 packets per second. For a similar simulation environment, e-AODV depicts an average throughput of just below 17000. The situation and the story is similar in the case of PDR

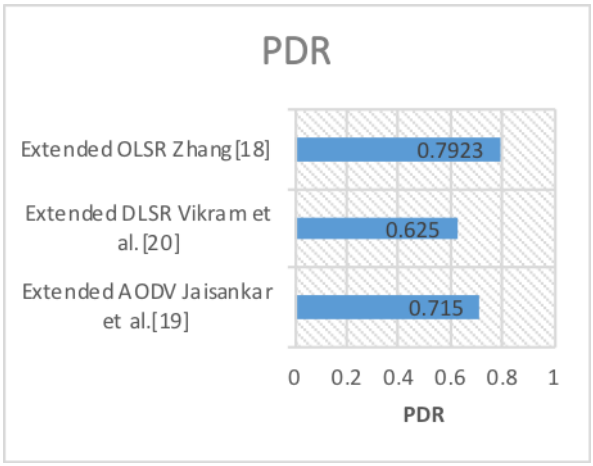

Fig. 6. PDR

V. CONCLUSION

MANETs and WSN have offered a wider platform to connect physical things digitally. The present review had summarized the traditional and some of the modified routing protocols that were published after the year 2010. Only the authenticated research publications that were published in Scopus, Google Scholar, IEEE, etc. were included in the study. The novel modifications and enhancement of traditional routing published in various papers directly show that the research community has been highly motivated to address the rising threats and security concerns of the society. Additionally, performance metrics have also been implemented by researchers to judge the quality of their

proposed designs quantitatively. The survey has been observed that the field of Ad-hoc mobile network is hastily growing, which requires strong routing mechanisms to address the present and the futuristic challenges.

REFERENCES

1. Biskupski, B., Dowling, J., & Sacha, J. (2007). Properties and mechanisms of self-organizing MANET and P2P systems. ACM Transactions on Autonomous and Adaptive Systems (TAAS), 2(1), 1.
2. Bang, A. O., & Ramteke, P. L. (2013). MANET: History, challenges and applications. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(9), 249-251.
3. Bellavista, P., Cardone, G., Corradi, A., & Foschini, L. (2013). Convergence of MANET and WSN in IoT urban scenarios. IEEE Sensors Journal, 13(10), 3558-3567.
4. Hasti, A. (2012). Study of impact of mobile ad hoc networking and its future applications. BIJIT-BVICAMs International Journal of Information Technology, 4(1), 439-444.
5. Gupta, R. (2011). Mobile Ad hoc Network (MANETS): Proposed solution to Security Related Issues. Indian Journal of Computer Science and Engineering (IJCSE), 2(5), 738-746.
6. Bruzgiene, R., Narbutaite, L., Adomkus, T., Ortiz, J. H., & de la Cruz, A. P. (2017). MANET network in internet of things system. Ad Hoc Networks, 89-114.

7. Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: imperatives and challenges. Ad hoc networks, 1(1), 13-64.
8. Kaur, H., Sahni, V., & Bala, M. (2013). A survey of reactive, proactive and hybrid routing protocols in MANET: A review. network, 4(3), 498-500.
9. Bakshi, A., Sharma, A. K., & Mishra, A. (2013). Significance of mobile AD-HOC networks (MANETS). International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2(4), 1-5.
10. Serhani, A., Naja, N., & Jamali, A. (2019). AQ-Routing: mobility-, stability-aware adaptive routing protocol for data routing in MANET–IoT systems. Cluster Computing, 1-15.
11. El-Tager, M., & Gadallah, Y. (2019, April). SWSP: Socially-Weighted Shortest Path Routing for Practical Internet of Things Applications. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.
12. Singla, V., Kakkar, P., & Lecturer, S. (2010). Traffic Pattern based performance comparison of Reactive and Proactive protocols of Mobile Ad-hoc Networks. International Journal of Computer Applications, 5(10), 16-20.
13. Kabir, T., Nurain, N., & Kabir, M. H. (2015, January). Pro-AODV (Proactive AODV): Simple modifications to AODV for proactively minimizing congestion in VANETs. In 2015 International Conference on Networking Systems and Security (NSysS) (pp. 1-6). IEEE.
14. Gandhi, S., Chaubey, N., Tada, N., & Trivedi, S. (2012, January). Scenario-based performance comparison of reactive, proactive & Hybrid protocols in MANET. In 2012 International Conference on Computer Communication and Informatics (pp. 1-5). IEEE.
15. Ravi, G., & Kashwan, K. R. (2015). A new routing protocol for energy efficient mobile applications for ad hoc networks. Computers & Electrical Engineering, 48, 77-85.
16. Rajaram, A., & Sugesh, J. (2011). Power aware routing for MANET using on-demand multipath routing protocol. International Journal of Computer Science Issues (IJCSI), 8(4), 517.
17. Vashistha, S. (2014). Improving the QOS in MANET by Enhancing the Routing Technique of AOMDV Protocol. In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I (pp. 381-392). Springer, Cham.
18. Zhang, D. G., Cui, Y. Y., & Zhang, T. (2019). New quantum-genetic based OLSR protocol (QG-OLSR) for Mobile Ad hoc Network. Applied Soft Computing, 80, 285-296.
19. Jaisankar, N., & Saravanan, R. (2010). An extended AODV protocol for multipath routing in MANETs. International Journal of Engineering and Technology, 2(4), 394.
20. Vikram, S. A., Afshar, A. M., & Bani, S. (2011). Quality of Service aware Dynamic Source Routing Protocol in Ad hoc Networks: Proposal, Analysis and Comparison. Computer Engineering and Intelligent Systems, 2(4), 211-221.
21. Ponguwala, M., & Rao, S. (2019). E2-SR: a novel energy-efficient secure routing scheme to protect MANET-IoT. IET Communications, 13(19), 3207-3216.
22. Alshehri, M. D., & Hussain, F. K. (2019). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing, 101(7), 791-818.
23. El-Semary, A. M., & Diab, H. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. IEEE Access, 7, 95185-95199.