ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse51842019.pdf
https://doi.org/10.30534/ijatcse/2019/51842019

Insights on Effectiveness of Secure Multicast Communication Scheme in Future Wireless Network

Ranjan Kumar H S[1, 2], Ganesh Aithal[3], Surendra Shetty[4]
[1]Department of CSE, NMAM Institute of Technology, Nitte, Karkala, India, ranjan@nitte.edu.in
[2]Research Scholar, VTU, Belagavi, India,
[3]Shri Madhwa Vadiraja Institute of Technology and Management, Udupi, India, ganeshaithal@gmail.com
[4]Department of MCA, NMAM Institute of Technology, Nitte, India, hsshetty@nitte.edu.in

ABSTRACT

With the increasing number of the ubiquitous application over the mobile network, the multicast communication system is the better option for boosting communication performance in the conventional wireless network. However, futuristic wireless network calls for significant changes in the multicast scheme while there is a significant issue to support potential security.

This paper offers comprehensive insights towards the usage of the multicast routing scheme with respect to offering security solution in the future wireless environment. The study finding of this investigation shows that there has been extensive usage of the multicast scheme, but the applicability of such scheme for a futuristic wireless communication system is highly restrictive as well as there was lack of consideration of dynamicity characteristics of adversaries.

The paper also contributes to highlighting the open research issues followed by significant points that are necessary to be considered while developing a secure multicast routing scheme in the future.

Key words: Wireless Sensor Network, Security, Key Management, Internet of Things, 5G, Multicast, Communication.

1. INTRODUCTION

Future wireless network comprises mainly of the concept of sensor networks and intelligent systems integrated with smart devices have received widespread attention from many different industries and research communities [1].The combination of sensor networks and intelligent devices is considered as the Internet of Things (IoT). This is due to a great effort by various researchers and development teams to bring continuous advancement and innovative approach to electronic technology which offers a variety of small-sized computing devices latched with sensing, data processing and communication module [2]. Currently, Wireless Sensor Networks (WSN) and IoT tech are playing their essential role in almost all areas ranging from education to healthcare systems, from services to production and from the government to private enterprises. A lot of research and development has been done in the WSN field, but it is not as attractive as the Internet of Things [3]. However, the concept of WSN can form an effective pillar for the IoT system and is undoubtedly an essential factor in the progress of IoT solutions. Therefore, collaboration between WSN and the IoT can provide a new paradigm for future sensor networks that will be inherently applied to daily human lives and make lives more comfortable. As no individual can think of their life and about work without the internet today, a day will come when the people cannot think of a single moment without the support of IoT.

Nowadays, the internet is mainly limited to PCs, laptops, smart devices, and digital other devices. However, the idea of a future sensor network is to allow things around us to interact with human as well as communicate with each other via the internet. However, there is a need for one-to-many communication mechanism in many applications, to achieve such a fully automated system of man and machine interaction. One-to-many communication in many applications is also often referred to as a multicast communication system which offers data transmission and messaging between resource-constrained sensors in IoT-enabled network. It also provides a cost-efficient mechanism by reducing bandwidth utilization, power, and computational overhead network terminals [4]. Although, a complete vision of future sensor network depends on many factors in which one of the main factors is associated with security and user privacy. As every person and sensor devices are connected to the Internet channel, are more vulnerable to privacy risk and various malicious attacks [5]. An attacker may compromise these devices illegally and steal data to use for their benefits and to perform unauthorized activities. In order to combat such security and privacy risk for secure multicast communication, a key management system is required [6]. A key management scheme act as a fundamental key for protecting group communications. Therefore, designing a secure key management scheme in parallel with a network framework design is crucial for achieving safe and reliable deployment of such advance IoT enabled automated sensor networks. Several efforts have been made recently in the research sector to solve issues related to key management [7-8].

This paper discusses the security traits of communication scheme in a future wireless network with emphasis on multicast routing schemes. Section 2 discusses the Futuristic

Wireless Architecture, followed by a discussion of security attacks on Section 3. Section 4 briefs about the multicast security aspects, while discussions of existing approaches are carried out in Section 5. Open research issues, are discussed in Section 6 while the conclusion is discussed in Section 7.

2. FUTURISTIC WIRELESS NETWORKS

Security and privacy are one of the most important factors in future sensor networks because it has the right to access personal user data and sensitive information that should be protected from unauthorized access and use. This section presents a layered architecture to understand many different security problems in IoT, shown in figure 1 [9].

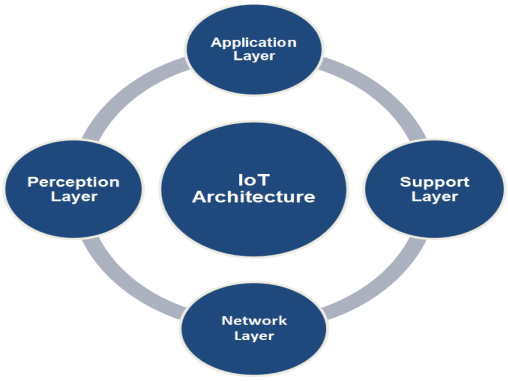

Figure 1: IoT-Sensor network Architecture

a) Application Layer

This layer allows the user to access IoT-enabled smart services based on their needs. In this user has the right to use different types of services using the application interface. Such services are a smart office, smart home, automated vehicle, and automated industrial system, smart healthcare, and various other automated systems.

b) Support Layer

This layer provides a viable platform for integrating IoT applications with other advanced systems such as cloud computing and fog computing. Here the fog computing node is used to provide hosting services for many applications, and cloud computing provide another computing resource as well as a huge data storage platform. The resources on this layer can be accessed through IoT devices through an internet channel.

c) Network Layer

The network layer is responsible for forwarding data collected from sensory layers or perceptual layers to the fog nodes, other IoT nodes, or to the cloud. This layer also ensures the protection of complete data transmission processes. On this layer, there are various network systems such as Ad-hoc networks, mobile Ad-hoc networks, and many more.

d) Perception layer

The perception layer is also known as the sensory layer, which includes wireless sensor devices, actuators, and RFID tags. These devices are the main components of this layer, which are responsible for sensing the surrounding environment, communicating between each other, and transmitting their collected data to the destination node.

3. SECURITY ATTACKS

This section discusses the possible security and privacy issues based on the layers of IoT infrastructure [10-11].

a) Application Layer Security

i). *Data Access*- Protecting data access at the application layer is a challenging issue because of the many user accessibilities with different privileges.
ii). *Phishing attacks*- Here, the attacker injects the malicious message to the steal user credentials and enables unauthorized access to the system login.

b) Support Layer

i). *Data Security*- In this layer, security issues related to data breaches, data fragmentation, and user privacy. In order to provide effective security to protect data in the cloud, there should be a mechanism to monitor system status, security, firewalls, and monitoring database login activity.
ii). *Portability*- The portability mechanism raises security issues in cloud systems. The portability between cloud providers is a key issue today. Different vendors use different standards that raise the challenge of migrating users from one to another. Therefore, this diversification also poses a security risk.
iii). *Cloud Audit*- The Security Association sets a number of standards for cloud providers that require continuous auditing to examine the protocols of these security policies to achieve and enhance user trust.

c) Network layer

i). Sybil Attack- Under this attack, a true node becomes a Sybil node, which declares its identity as a true node in the deployment area. This type of attack can have a very harmful effect on the entire routing process of the network.
ii). *DoS Attack*- Denial of service attack is also a kind of rude attacks which makes service of whole network system unavailable by flooding unnecessary traffic for certain period so that an adversary can steal information using some another approach at the same time.
iii). *Routing attack*-In this case, the attacker creates fake routing information between intermediate nodes to obtain false information or burst routing loops so that a malicious person can acquire data during data transmission from the source to the destination.
iv). *Eavesdropping Attack*- This type of attack is also known as a spoofing attack, in which a malicious user silently monitors the traffic and communication patterns of the network system. They capture all the necessary information without performing any other attacks.

d) Perception layer

In this layer, an attacker performs an attack on the node in the deployment area and tries to gain physical access over the nodes. Once the nodes are compromised the attacker can destroy the whole network by destroying sensor nodes or manipulating functions of sensor nodes

4. SECURING MULTICAST IN FUTURE WIRELESS NETWORK

Multicast communication is a proficient method for appropriating data to a group of members. As opposed to unicast communications, multicast routing licenses a solitary IP datagram to be routed to numerous hosts at the same time. Participation in a multicast group is dynamic, enabling hosts to enter and leave the multicast session without the consent or information of different hosts. The characteristic advantages of multicast routing may likewise show a few vulnerabilities making it helpless to assault except if they are verified. The objective is to verify these vulnerabilities while keeping up the advantages of multicast administration.

The field of applying multicast is as complex as the application zone of IoT itself; including smart homes, smart urban communities, ecological checking, and medicinal services. For a superior comprehension of significant prerequisites for a multicast bolster, the accompanying two use cases are resolved.

The primary use case is intended for the control of light bulbs in a smart structure and is shown in Figure 2. The natural observing network gathers data about light force, temperature, and populace of all rooms in the structure and conveys amassed data to a focal substance. In light of data got, the focal element can empower synchronous tasks (e.g., giving directions for on, off, or diminish level) among a group of light bulbs in a story or space to achieve visual synchronicity of light impacts on the client.

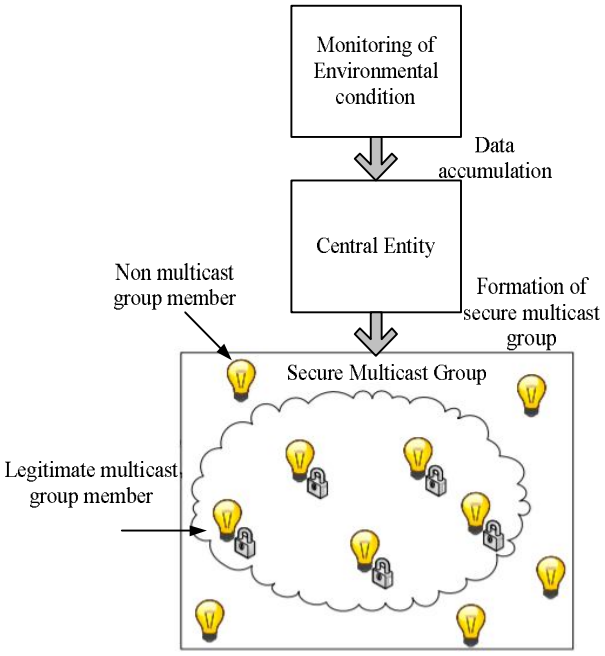

Figure 2: Creation of multicast group for bulb system

The subsequent use case is about the accumulation and total of patient data and conveying the data required to significant contacts (e.g., specialists or medical attendants), which is represented in Figure 3. The amassing unit gathers data about the patient's ECG readings and pulse. Like this, the preparing unit decides the precise arrangement of members, who ought to respond as per the data gained, and characterizes them as a novel multicast group. In these two use cases, multicast groups must be safely shaped individual mystery keys must be shared among all multicast group individuals to guarantee secure communications.

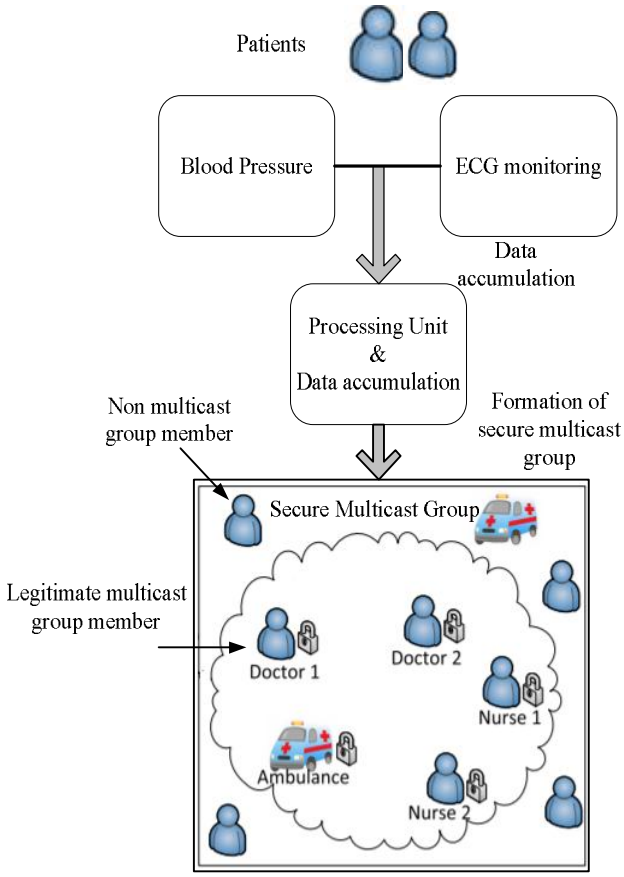

Figure 3: Creation of the multicast group for health care

Recently, the research community has produced various forms of the applicability towards the various applications such as healthcare, monitoring of the environment, smart home monitoring, etc. With these advancements, most of the users are highly dependent on day today life, and hence, the security and privacy are becoming a major concern. Also, the existence of complex as well as the dynamic nature of the data formation in IoT is introducing a lot of challenges in the security concerns. The existing wireless nodes are having a lot of resource constraints, which is generating a lot of security issues and leading to necessary of lightweight security solution [12]. A multicast system has the feature of data transfer through a symmetric-based encryption algorithm, which is very lighter to offer the reliable, simple computational ability for the security concerned IoT applications. However, a challenging situation is the better distribution of the security key for the group members for the dynamic characteristic aware IoT applications.

5. EXISTING APPROACHES

At present, there are various research works towards the usage of multicast communication approaches in futuristic wireless

networks. The usages of multicast routing scheme in existing approaches are mainly focused on communication and resource efficiency. Although the majority of the categories of existing research work are not directly linked up with the security system, their features are most important in order to support a robust security system. It has been explored recently that network coding could significantly escalate the working operation of the multicasting system. The study carried out by Chen et al. [13] has used multicasting of packets over cognitive network considering network coding of arbitrary type. Some of the contributions of this study are that it offers a significant reduction in effort to transmit data as well as gain in receiving data. The information to be decoded is potentially reduced to a greater extent. This study contributes to the fact that network coding could significantly support the applicability of network security protocols. Study towards the usage of network coding has also been reported in the work of Li et al. [14]. The presented study has used a cross-layer based approach focusing on beam forming while the network layer is subjected to network coding of random type and adaptive nature.

The work of Wang et al. [15] has been used encryption approach with the network coding for further accelerating the security protocols. The authors have used allocation for routing and spectrum protocol for sorting out the issue of integer linear programming model over the optical network as a case study of the network. According to the authors, it was said that the optimization of both unicast and multicast protocol using network coding offer better communication services. Adoption of device-to-device communication over using hybrid multicasting has been carried out by Li et al. [16] where similar adaptive network coding using arbitrary type has been used. The study also discusses the packet scheduling scheme that is claimed to offer better network throughput. A similar statement of research work has also been given by Chu et al. [18] where the author has connected resource factor with the security aspect of multicast communication services in the wireless network. The author has emphasized on the power factor using jointly unicast and multicasting system. A mathematical approach has been used for solving this problem in the study where the outcomes have been claimed to achieve better secrecy performance over the different rate of multicast in the adverse scenario of communication. A joint investigation over multicast and unicast operation has also been carried out by Guo et al. [19] where a hybridized scheme has been used. The authors have used the genetic algorithm as well as a greedy approach in order to perform optimization of the streaming services over the wireless network. Although this study has no direct implementation of a security system, it offers a scheme where heavier file system over a streaming network could be transmitted through various dedicated channels with low resource consumption. Such an environment could be an ideal environment of implementing distributed key management system.

Majority of the upcoming wireless networks calls for resource-efficient security algorithm usage otherwise the security features, as well as communication capability, couldn't be enhanced at the same time. The work carried out by Li et al. [20] have used a mechanism that can generate a symmetric secret key in order to secure the group based communication system. The investigation has been carried out considering the case study of wireless body area network. The approach uses received signal strength indicator for the generation of the symmetric key using multicasting operation. Existing studies also discuss the key distribution scheme using both multicasts as well as a unicast transmission scheme. The work carried out by Ganesan et al. [21] has used a discrete work allocation for both unicasting and multicasting. The unicasting was used for secure generation of the key while the distribution of the secret key is carried out by multicasting operation without any dependency to perform encryption. The study also claimed of controlling the communication cost owing to adoption of tree-based management of key.

The group key management for securing the wireless network is noticed in state of art of research. Such direction of the work has been carried out by Halford et al. [22] where key agreement scheme has been presented. The authors have implemented public key encryption considering the energy efficiency factor along with it. The study also performs a characterization of the session key for boosting the encryption process. Study towards group key based secure multicasting communication has been carried out by Porambage et al. [23] where the Internet-of-Things (IoT) environment has been considered. The implementation makes use of a network and adversary model followed by a signal scheme (elliptical curve). The study outcome showed that the cost of energy is significantly under control. Schemes of security management using group key have been carried out by Baddi and Kettani [24]. The authors have used a tree-based approach for constructing the communication system considering the mobile networks environment. The study deals with forwarding the secret key over multicast scheme using this topology. However, it should be noted that existing key management protocols are reported to have lower applicability towards many numbers of groups exercising multicast protocols. This problem has been addressed by Mapoka et al. [25] where slot-based management of group key is used. The work is reported to assist in mobile communication between both single and multiple numbers of users over different domains of the wireless network. The outcome of this work is also claimed to control the overheads caused due to rekeying transmission. Apart from this, the study also reported to have better control over the channel capacity as well as resource conservation too. The applicability of this work is also discussed with mobile wireless networks with multicasting approach.

In order to implement an excellent security-based solution towards the multicast-based communications system over the wireless network, it is required to offer multiple characteristics. At present, various researchers have presented certain techniques in order to offer better supportability of complex algorithm execution, e.g., encryption. One of such

objectives has been included in the work of Al-Dubai et al. [26] where the scalability problem is addressed. In order to develop a robust security scheme, the system should offer high-end scalability. The study has implemented an inter-domain routing scheme where multicasting has been used for offering a solution towards ubiquitous connection in the wireless network. Inclusion of multicast over the multihop network was also another important consideration to develop an effective security protocol with better throughput. Study in such direction has been carried out by Luo et al. [27] where analytical modeling has been constructed in order to design a communication scheme using multicast. The authors have also used the stochastic approach in order to perform modeling. Study towards multiple multicasting protocols has also been carried out by Park et al. [28] where a group key management technique has been discussed that use asymmetric keys. According to this concept, the authors have used one master key and a various number of secret slaves key. These keys are generated by the presented approach that can increase the security features. Another advantageous feature is that it maintains better cost-effectiveness by ensuring that updating process of one key leads to autonomous updating process for others. The study outcome is proven to offer reduced overhead towards its storage.

The upcoming network system is also reported to use millimeter wave for faster transmission by offering superfluous channel capacity. An effective, secure communication system will also need a better scheduling scheme so that security, as well as transmission, can be well synchronized. Research in such direction was carried out by Niu et al. [29] where a unique scheduling scheme has been presented over a millimeter wave using multicasting approach. The scheme also uses codebooks of multiple levels considering device-to-device communication. The study outcome showed that it offers reduced energy consumption and better network throughput. The next generation of wireless networks calls for extensive usage of 5G, which has different types of multiple access techniques. Non-Orthogonal multiple access or NOMA is one such access technique used in the 5G network, and it is believed to improve upon the user reliability. Similar utilization of the NOMA was also seen in the work of Zhao et al. [30] with better supportability of the multicasting protocols as well as resource allocation. The authors have also investigated the outage performance of the presented scheme. The study outcome shows that it offers increasing data rate over communication channels with artifacts. Apart from this, it is also proven to offer the reduced probability of outage, which will mean that this mechanism is well suited for running authentication protocol over a future wireless network with ease. Study towards such direction has been carried out by Yang et al. [31] where a discrete mechanism of forwarding the information has been formulated with respect to both unicast as well as the multicast user. The study contributes to overcoming the security loopholes by addressing the outage problem using a probability-based model. Similar adoption of NOMA was also seen in the work of Zhang et al. [32] where the focus was mainly towards communication between different groups of multicast. The simulated outcome of the study shows that spectral efficiency has been improved while there is a good outcome for better system coverage too. The work carried out by Zhang et al. [33] has contributed a study that focuses on the heavy transmission of content over the multicast communication channel considering the fading problems incorporated within it. According to the author, plying a cross-layered based approach integrated with the allocation of power scheme in the wireless network could offer better adaptability. This characteristic of adaptability could be significantly used for developing and supporting distributed security algorithm without affecting the quality of the contents being transmitted. The study carried out by Zhang et al. [34] has also used the millimeter wave where multicasting protocol has been implemented over a heterogeneous network. The author has used a unique search strategy for performing optimization targeting the energy efficiency part of it. It is because the implication of the energy efficiency could only confirm better utilization of the allocation of energy with better transmission capability that is essential for running any cryptographic algorithm. Therefore, although the authors have not used cryptographic algorithm then also their objectives of the study are in good supportability of the encryption algorithms over millimeter wave using stochastic geometry. Multicasting mechanism was also implemented for the heterogeneous network by Zhou et al. [35] where network virtualization has been considered for video transcoding. Study towards multi-cell and multicast protocols has been carried out by Zhou et al. [36].Table 1 summarizes the category of techniques mentioned in figure 4

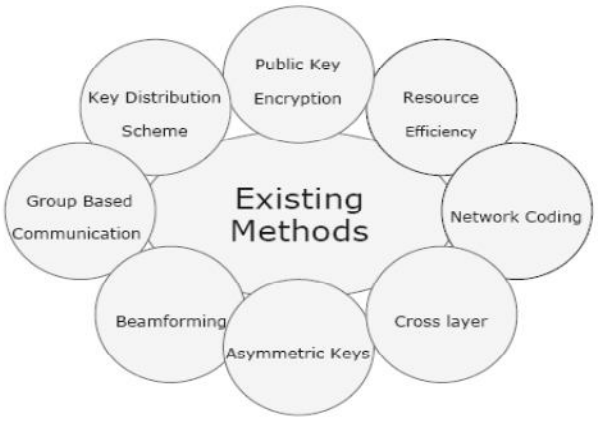

Figure 4: Existing Approaches of Secure Multicasting

Table 1: Summary of Existing Approach

Authors	Problems	Techniques	Performance	Outcome
Chen et al. [12]	Packet Multicast	Simulation	Base_LinkSuc, Packet Transmitted	Presents packet multicast method into the CRAHNs.
Chu et al. [16]	Secure wireless powered Unicast services, Multicast Integrated.	Experimental	Multicast cost, Secrecy cost	Numerical outcomes are given to authenticate the proposed method.
Guo et al. [17]	Mobile multimedia services	Simulation	Average PSNR, Least Stability Index	Resource allocation approach for the many transport expertise
Li and Fang [18]	Lightweight, Resource effectiveness security approach	Experimental	Fault rejection rate, Variation tolerance	Enhances the Symmetric key-generation technique
Li et al. [13]	Enhance the performance of the wireless multicast network	Analytical	Transmitting power, Network Throughput	Sends HDCP multimedia data to users over make sure channels by using BS.
Li et al. [15]	D-2-D Transmission Method, Hybrid Multicast	Analytical	Timeslot Deadline, Network Throughput	Corroborate the efficiency of the proposed methods.
Ganesan et al. [19]	Secure Key Allocation	Experimental	Dynamic users, Encryptions	The outcome illustrates the non encrypted transmission for secure group statement in wireless IP-v6 n/w using PMUKD method.
Halford et al. [20]	Group key agreement	Experimental	Group Size, Group Key	public key algorithm
Prambage et al. [21]	Key management for security, energy	Experimental	Network size, energy	Performs good authentication
Baddi and KEttani [22]	Group key organization over the internet	Simulation	Multicast group size, Encryption procedures	Reduction in encrypt and decrypt operations and another feature.
Wang et al. [14]	Formulation of RSA Algorithm for the for the hybrid n/w coding	Simulation	Receivers, Range of resources	RSA approach on flexible visual network for the hybrid services.
Mapoka et al. [23]	Novel multiple service key management	Analytical	Multicast services, communication overhead	An enhancement of the performance of key management
Al-Dubai et al. [24]	Quality of Service-Aware multicast	Experimental	Packet/Second, Standardized value	Presents a new multicast policy to handle QoS-aware function into the WCN.
Luo et al. [25]	Throughput of Non-asymptotic	Analytical	Receivers, Delay	The models are drawn with further verification and correctness of the systematic bound.
Park et al. [26]	Key management in the mobile multicast communication	Analytical	Multicast services, communication overhead	An enhanced key management and improvesperformance in multi-group provisions
Niu et al. [27]	An efficient multicast planning method	Experimental	Users, Throughput	A significant enhancement in network throughput, energy effectiveness contrasted with a different state of the art methods.
Yang et al. [29]	Presents a new non-orthogonal multiple access	Analytical	System SNR, Outage throughput	Validates the theoretical outcomes, benefits of the proposed corporation plan
Zhang et al. [30]	Enhance the performance into the throughput, coverage	Analytical	SINR, Frequency	Get intergroup cooperation between MGs which is known as COM-NOMA technique
Zhang et al. [31]	Improve video broadcast design	Simulation	SNR, PSNR	Cross-layer demonstrated for the wireless video multicast methods

Zhang et al. [32]	Achievement of multicast mm-wave wireless n/w	Analytical	Power distribution issue, multicast price	Shows that the NOMA may considerably enhance the mmWave multicasting
Zhao et al. [33]	Decline the range efficiency using NOMA Technique	Analytical	Typical SNR, Outage probability	An authenticated systematic outcome, shows the performance expands of NOMA-MC method
Zhou et al. [34]	Present a framework of virtualized heterogeneous n/w	Analytical	Groups of multicast, MVNO utility	The outcome shows the efficiency of the proposed method
Zhou et al. [35]	Design of cache-aware multicast beamforming	Experimental	Storage space, communication power	Demonstrates the robust joint optimization policy for the defective channel state information to support the stabilization of the method.

6. OPEN RESEARCH ISSUES

From the prior section, it has been seen that there are various studies being carried out towards securing multicast communication protocol in future wireless network. Existing studies in a large extent have addressed security and compatibility of those security algorithms; however, there are certain areas which are yet to be addressed effectively and those are yet an open end problems. The highlights of the open research issues are as follows.

- *Higher Unpredictability*: Adoption of multicasting communication calls for transmitting the data to selected recipient. However, upcoming 5G networks offer supportability to ad hoc network also. Therefore, there is no solution yet existing to even find out the source of receiving such multicast data packets. This offers greater deal of unpredictability about the genuinity of the mobile nodes under any form of futuristic wireless network.
- *Low Strength Key Management*: The state of art has reportedly experimented with different form of encryption mechanism mainly using key management. However, the formation of key management is highly conventional manner and there is less number of attributes to maintain proper secrecy of such generated keys. The upcoming types of wireless communication system definitely calls for such keys to work in distributed manner while the existing system doesn't offer any claim that such approaches are applicable over distributed and large scale future wireless networks.
- *Lack of Identifying Malicious Intention*: None of the existing studies are framed up with a concept of dynamic attack that is highly feasible when a wireless network is connected with large connected network like internet (example is device-to-device communication, IoT, etc) [37]. All the existing approaches of securing multicast protocols are based on apriori information about the attackers which is quite inapplicable in case of large ubiquitous wireless network. In such case, there should be capability to identify adversaries and offer necessary solution to resist it. IoT is powered by potential data analytics which can do this job, however, such analysis for attackers should happen instantly in order to identify and stop the attack.
- *Less Computationally Intensive Algorithm*: Some approaches towards securing multicast routing protocols are found to offer either a complex encryption operation or a sophisticated routing scheme. Such operation are not yet claimed to be friendly with the resource constrained devices (like devices in IoT). Offering a good balance between energy efficiency as well as other resource efficiency using extremely light weight key management operation is significantly missing in existing system.

7. CONCLUSION

This paper has discussed the security aspect connected with the multicast routing policies associated with the futuristic wireless communication system. After reviewing an existing approach following the findings of the study is obtained:

- Existing studies contribute to show its applicability towards secure multicasting considering the case study of millimeter wave as well as different multiple access techniques of the upcoming 5G networking system. However, such consideration of the futuristic network has not been investigated with respect to dynamic attacks whose possibilities are exponentially high.
- The present system has less number of encryption algorithm used for securing multicast routing schemes. There is also good evidence of the studies using a non-cryptographic approach that offers better supportability towards encryption algorithm. However, they have never being experimented or studied in such a non-cryptographic approach. Therefore, there is a need for a lightweight encryption algorithm that can offer a robust balance between security as well as communication performance for any form of the futuristic wireless network of dynamic type.
- All the existing approaches are based on frequently used approaches, e.g., resource efficiency, network coding, cross-layer, beam forming, hybrid multicasting,

group-based communication, tree-based management of key, public key encryption, rekeying, asymmetric keys, etc. However, there is also a need for more comprehensive protocol towards resisting dynamic attacks.

REFERENCES

1. Čolaković A, Hadžialić M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks. 2018 Jul 20. https://doi.org/10.1016/j.comnet.2018.07.017
2. Sethi, Pallavi, and Smruti R. Sarangi. "Internet of things: architectures, protocols, and applications." Journal of Electrical and Computer Engineering 2017 (2017). https://doi.org/10.1155/2017/9324035
3. Ray, Partha Pratim. "A survey on Internet of Things architectures." Journal of King Saud University-Computer and Information Sciences 30.3 (2018): 291-319. https://doi.org/10.1016/j.jksuci.2016.10.003
4. Park, Jiye, Markus Jung, and Erwin P. Rathgeb. "Survey for Secure IoT group communication." 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2019. https://doi.org/10.1109/PERCOMW.2019.8730750
5. Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312. https://doi.org/10.1109/COMST.2015.2388550
6. Yu, Hong, et al. "A group key distribution scheme for wireless sensor networks in the internet of things scenario." International Journal of Distributed Sensor Networks 8.12 (2012): 813594. https://doi.org/10.1155/2012/813594
7. Renugadevi, N., G. Swaminathan, and Aditya S. Kumar. "Key management schemes for secure group communication in wireless networks-a survey." 2014 International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2014. https://doi.org/10.1109/IC3I.2014.7019627
8. Vasala, Uma, and Dr GR Sakthidharan. "Effective Key Management In Dynamic Wireless Sensor Networks." International Journal of Computer Engineering in Research Trends 4.7 (2017): 308Y312.
9. G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010
10. Ahemd, Mian Muhammad, Munam Ali Shah, and Abdul Wahid. "IoT security: A layered approach for attacks & defenses." 2017 International Conference on Communication Technologies (ComTech). IEEE, 2017. https://doi.org/10.1109/COMTECH.2017.8065757
11. El Mouaatamid, Otmane, Mohammed Lahmer, and Mostafa Belkasmi. "Internet of Things Security: Layered classification of attacks and possible Countermeasures." Electronic Journal of Information Technology 9 (2016).
12. Deepti Sehrawat, Nasib Singh Gill " A Review on Performance Evaluation Criteria and Tools for Lightweight Block Ciphers" International Journal of Advanced Trends in Computer Science and Engineering, Vol.8 no. 3 pp. 630-639. https://doi.org/10.30534/ijatcse/2019/47832019
13. B. Chen *et al*., "Packet Multicast in Cognitive Radio Ad Hoc Networks: A Method Based on Random Network Coding," in *IEEE Access*, vol. 6, pp. 8768-8781, 2018. https://doi.org/10.1109/ACCESS.2018.2805762
14. B. Li, X. Li, R. Zhang, W. Tang and S. Li, "Joint Power Allocation and Adaptive Random Network Coding in Wireless Multicast Networks," in *IEEE Transactions on Communications*, vol. 66, no. 4, pp. 1520-1533, April 2018. https://doi.org/10.1109/TCOMM.2017.2785238
15. Xin Wang, Ren-Tao Gu and Y. Ji, "RSA for the hybrid unicast and network coding based multicast services over the flexible optical networks," *2016 25th Wireless and Optical Communication Conference (WOCC)*, Chengdu, 2016, pp. 1-4. https://doi.org/10.1109/WOCC.2016.7506621
16. [15] B. Li, H. Li, X. Li, H. Jiang, W. Tang and S. Li, "Hybrid Multicast and Device-to-Device Communications Based on Adaptive Random Network Coding," in *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2071-2083, March 2019. https://doi.org/10.1109/TCOMM.2018.2882797
17. Z. Chu *et al*., "Resource Allocation for Secure Wireless Powered Integrated Multicast and Unicast Services With Full Duplex Self-Energy Recycling," in *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 620-636, Jan. 2019. https://doi.org/10.1109/TWC.2018.2883563
18. J. Guo, X. Gong, J. Liang, W. Wang and X. Que, "An Optimized Hybrid Unicast/Multicast Adaptive Video Streaming Scheme Over MBMS-Enabled Wireless Networks," in *IEEE Transactions on Broadcasting*, vol. 64, no. 4, pp. 791-802, Dec. 2018. https://doi.org/10.1109/TBC.2018.2832444
19. [Z. Li, H. Wang and H. Fang, "Group-Based Cooperation on Symmetric Key Generation for Wireless Body Area Networks," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1955-1963, Dec. 2017. https://doi.org/10.1109/JIOT.2017.2761700
20. V. C. Ganesan, A. Periyakaruppan and R. Lavanya, "Cost-effective polynomial-based multicast–unicast key distribution framework for secure group

communication in IPv6 multicast networks," in *IET Information Security*, vol. 10, no. 5, pp. 252-261, 9 2016.
https://doi.org/10.1049/iet-ifs.2015.0398

21. T. R. Halford, T. A. Courtade, K. M. Chugg, X. Li and G. Thatte, "Energy-Efficient Group Key Agreement for Wireless Networks," in *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5552-5564, Oct. 2015.
https://doi.org/10.1109/TWC.2015.2439675
22. P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila and B. Stiller, "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications," in *IEEE Access*, vol. 3, pp. 1503-1511, 2015.
https://doi.org/10.1109/ACCESS.2015.2474705
23. Y. Baddi and M. D. E. E. Kettani, "Optimal Shared Multicast Tree Based Solution for Group Key Management in Mobile IPv6," *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, Marrakech, 2018, pp. 567-572.
https://doi.org/10.1109/CIST.2018.8596622
24. T. T. Mapoka, S. J. Shepherd and R. A. Abd-Alhameed, "A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast," in *IEEE Transactions on Mobile Computing*, vol. 14, no. 8, pp. 1545-1559, 1 Aug. 2015.
https://doi.org/10.1109/TMC.2014.2362760
25. A. Y. Al-Dubai, L. Zhao, A. Y. Zomaya and G. Min, "QoS-Aware Inter-Domain Multicast for Scalable Wireless Community Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 11, pp. 3136-3148, 1 Nov. 2015.
https://doi.org/10.1109/TPDS.2014.2365190
26. J. Luo, L. Yu, J. Zhang and X. Wang, "Nonasymptotic Multicast Throughput and Delay in Multihop Wireless Networks," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5525-5537, July 2016
https://doi.org/10.1109/TVT.2015.2465963
27. M. Park, Y. Park, H. Jeong and S. Seo, "Secure Multiple Multi-cast Services in Wireless Networks," in *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1712-1723, Sept. 2013.
https://doi.org/10.1109/TMC.2012.135
28. Y. Niu, L. Yu, Y. Li, Z. Zhong and B. Ai, "Device-to-Device Communications Enabled Multicast Scheduling for mmWave Small Cells Using Multi-Level Codebooks," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2724-2738, March 2019.
https://doi.org/10.1109/TVT.2018.2883641
29. Z. Zhao, M. Xu, Y. Li and M. Peng, "A Non-Orthogonal Multiple Access-Based Multicast Scheme in Wireless Content Caching Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2723-2735, Dec. 2017.
https://doi.org/10.1109/JSAC.2017.2726698
30. L. Yang, J. Chen, Q. Ni, J. Shi and X. Xue, "NOMA-Enabled Cooperative Unicast–Multicast: Design and Outage Analysis," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 7870-7889, Dec. 2017.
https://doi.org/10.1109/TWC.2017.2754261
31. Y. Zhang, X. Wang, D. Wang, Y. Zhang, Q. Zhao and Q. Deng, "NOMA-Based Cooperative Opportunistic Multicast Transmission Scheme for Two Multicast Groups: Relay Selection and Performance Analysis," in *IEEE Access*, vol. 6, pp. 62793-62805, 2018.
https://doi.org/10.1109/ACCESS.2018.2876598
32. Z. Zhang, D. Liu, X. Ma and X. Wang, "ECast: An Enhanced Video Transmission Design for Wireless Multicast Systems Over Fading Channels," in *IEEE Systems Journal*, vol. 11, no. 4, pp. 2566-2577, Dec. 2017.
https://doi.org/10.1109/JSYST.2015.2438071
33. Z. Zhang, Z. Ma, Y. Xiao, M. Xiao, G. K. Karagiannidis and P. Fan, "Non-Orthogonal Multiple Access for Cooperative Multicast Millimeter Wave Wireless Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 8, pp. 1794-1808, Aug. 2017.
https://doi.org/10.1109/JSAC.2017.2710918
34. Z. Zhao, M. Xu, Y. Li and M. Peng, "A Non-Orthogonal Multiple Access-Based Multicast Scheme in Wireless Content Caching Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2723-2735, Dec. 2017.
https://doi.org/10.1109/JSAC.2017.2726698
35. Y. Zhou, F. R. Yu, J. Chen and Y. Kuo, "Video Transcoding, Caching, and Multi-cast for Heterogeneous Networks Over Wireless Network Virtualization," in *IEEE Communications Letters*, vol. 22, no. 1, pp. 141-144, Jan. 2018.
https://doi.org/10.1109/LCOMM.2017.2759780
36. Y. Zhou, F. R. Yu, J. Chen and Y. Kuo, "Cache-Aware Multicast Beamforming Design for Multicell Multigroup Multicast," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11681-11693, Dec. 2018.
https://doi.org/10.1109/TVT.2018.2872966
37. Sasi Bhanu, JKR Sastry,Venkatesh Sunil Kumar,Venkatesa Sai,K V Sowmya, " Enhancing Performance of IoT Networks through High Performance Computing", International Journal of Advanced Trends in Computer Science and Engineering Vol.8 no. 3 pp. 430-442