Websites:
http://www.sciencepub.net/academia
http://www.sciencepub.net

Emails:
aarena@gmail.com
editor@sciencepub.net

Academia Arena

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

# Review Of Literature Related To The Study On The Routing In Networking

*Prof. Rajeev Yadav and ** Reenu Goyal

* Professor, Department of Computer Science, OPJS University, Churu, Rajasthan (India)
**Research Scholar, Department of Computer Science, OPJS University, Churu, Rajasthan (India)
Email: renu12goel@gmail.com

**Abstract:** Routing is playing a vital role in IoT devices. Routing is a very challenging aspect that takes place in IoT because of its intrinsic properties. Sometimes routing protocol called as routing policy, which specifies how routing devices communicate with each other in the network, circulating control information that to select best routes between any two nodes among multiple routes. In routing protocol information (or) data can be shared from a source node through nearest neighbors and reaches to the sink node. Based upon algorithms in routing it decide the best path between the source and the destination node. Different authors implemented different algorithms and protocols to increase the lifetime of the network, efficiency in routing. Wireless Sensor Networks (WSNs) consists of densely deployed wireless sensor nodes which does the task of sensing the environment in which they are placed. Due to high density nature of these nodes there is a need for an efficient routing algorithm for transferring data from the source node to the sink by choosing the best possible path. The nodes in a particular area transfer data to the Base Station (BS). The base station acts as a gateway for the user to query the environment in which they are placed. The routing protocols adapted for wireless sensor networks are either traditional single layered MAC protocols or cross-layer protocols which enable interaction between different layers of the OSI model. Some traditional geographic routing protocols make use of GPS or other localization techniques to determine their position. The review is achieved through research papers based solely on geographic and cross-layer routing.
[Yadav, R. and Goyal, R. **Review Of Literature Related To The Study On The Routing In Networking.** *Academ Arena* 2020;12(7):4-7]. ISSN 1553-992X (print); ISSN 2158-771X (online). http://www.sciencepub.net/academia. 2. doi:10.7537/marsaaj120720.02.

**Keywords:** review of literature, **routing, networking**

## Introduction:

Network routing algorithms responsible for selecting paths to destinations have a profound impact on network stability experienced by the network users. Unfortunately, performance of state-of-the-art routing algorithms often falls short of users' expectations. (i) The flexibility with which operators of independently administered networks can choose their routing policies allows them to make selections that are conflicting and may lead to route cycles. Oscillating routes have a negative impact on performance experienced by the user, and also cause overloading of the routers with control messages. (ii) Interdomain routing in the Internet is based on trust. As a result, false route announcements can be made by a malicious network operator. Such false announcements can be made even without knowledge of the network operator, due to accidentally misconfigurations or router hijacking. False route announcements may lead to denial of service, or worse yet; traffic can be intercepted without detection of both the sender and recipient. (iii) Even if network routes are stable and secure, unexpected equipment failures may cause performance degradation. It is difficult to preconfigure current routing protocols with all possible failures in mind, and not enough exibility is offered to balance load in the network evenly. In the past years several research papers have done studies to explore these areas of prefix hijacking, cycles and traffic engineering with load balancing.

## Review of literature

As suggested earlier, exploratory search can describe either the problem context that motivates the search or the process by which the search is conducted (Marchionini, 2006a). Kent et al (2000). This Study describes the results of these experiments – examining interoperability, the efficacy of the S-BGP countermeasures in securing BGP control traffic, and their impact on BGP performance, and thus evaluating the feasibility of deployment in the Internet In addition to the security-related benefits to be gained, performance considerations are crucial in convincing users and vendors to adopt the S-BGP countermeasures and deploy them into the Internet. This experiment with a prototype implementation and real-world BGP traffic supported prior analysis results which indicated

that the overhead added by the S-BGP countermeasures needed the CPU/memory equivalent of a desktop PC. A number of techniques can be used to enable the BGP speakers to handle spikes in the UPDATE traffic. This includes use of auxiliary processors, deferral of route validation until a route is needed, and offloading of certificate and AA (address attestations) processing. CPU — Although caching of recent route data should enable a speaker to avoid the need to validate approximately 53% of UPDATEs, testing showed that a DSP might see little benefit from caching. However, the UPDATE arrival rate in such circumstances is sufficiently low to mitigate CPU utilization concerns anyway. In contrast, an S-BGP speaker at a NAP would benefit considerably from caching, based on analysis of Merit data. Cryptographic hardware could be added to handle the signature and verification tasks, but high speed signature algorithm software, e.g., the Open SSL distribution, provides very good performance. CPU requirements for processing certificates and AA are addressed by having organizations/ASes handle this processing and using an out-of-band distribution of certificates and AAs to all S-BGP speakers. Bandwidth — the increased transmission bandwidth required by S-BGP on a steady-state basis represents a small amount of data relative to subscriber traffic. In addition, a number of optimizations have been adopted to minimize overhead – the encoding scheme used for attestations, the choice of signature algorithm, and the use of certificate and AA extracts. Even at initialization, the time required to transmit certificates and AAs for the full Internet routing table is minimal. 21 M. Lad et al (2006). This study presents a new Prefix Hijack Alert System (PHAS). PHAS is a real-time notification system that alerts prefix owners when their BGP origin changes. In a BGP prefix hijacking event, a router originates a route to a prefix, but does not provide data delivery to the actual prefix. Prefix hijacking events have been widely reported and are a serious problem in the Internet. By providing reliable and timely notification of origin AS changes, PHAS allows prefix owners to quickly and easily detect prefix hijacking events and take prompt action to address the problem. This illustrates the effectiveness of PHAS and evaluates its overhead using BGP logs collected from RouteViews. PHAS is light-weight, easy to implement, and readily deployable. In addition to protecting against false BGP origins, the PHAS concept can be extended to detect prefix hijacking events that involve announcing more specific prefixes or modifying the last hop in the path. In this Study the design of PHAS is described, a Prefix Hijack Alert System. Rather than attempting an accurate route hijacking detection algorithm, PHAS aims at providing timely notification of origin AS changes to the owners of individual prefixes in a reliable way. The prefix owners can then easily identify real hijack alerts and filter out normal origin changes. By avoiding running complex data processing at BGP data collectors, PHAS can be quickly implemented and run with little overhead at the data collectors. By automating the email processing at the user end, PHAS provides network operators with real-time alerts to potential prefix hijacks while adding virtually no overhead to the operation tasks. PHAS leverages on the existing routing logs for data input and the universally available email system for notification delivery. PHAS is light on authentication of users because its information is derived from publicly available data, and is light on data filtering because it simply provides information to users for hijack detection. As a result PHAS is light weight and readily deployable. As next step it is planned to implement and install PHAS at RouteViews for trial deployment. Oorschot et al (2007). This study, presents Pretty Secure BGP (psBGP)—a proposal for securing BGP, including an architectural overview, design details for significant aspects, and preliminary security and operational analysis. It is well known that the Border Gateway Protocol (BGP), the IETF standard Interdomain routing protocol, is vulnerable to a variety of attacks, and that a single misconfigured or malicious BGP speaker could result in large-scale service disruption. psBGP differs from other security proposals (e.g., S-BGP and soBGP) in that it makes use of a single-level PKI for AS number authentication, a decentralized trust 22 model for verifying the propriety of IP prefix origin, and a rating-based stepwise approach for AS_PATH (integrity) verification. psBGP trades off the strong security guarantees of S-BGP for presumed-simpler operation, e.g., using a PKI with a simple structure, with a small number of certificate types, and of manageable size. psBGP is designed to successfully defend against various (non-malicious and malicious) threats from uncoordinated BGP speakers, and to be incrementally deployed with incremental benefits. Beyond AS_PATH verification, it is desirable to verify if an AS_PATH conforms to the route-exporting policies of each AS on the path. Since BGP is a policy-driven routing protocol, each AS can individually decide whether or not a received route advertisement should be further propagated to a neighboring AS. Such route-exporting policies are mainly defined based on the business relationship with a neighboring AS. Without such verification, a misbehaving BGP speaker (e.g., misconfigured) may be able to re-advertise routes which are prohibited by its route-exporting policies. A multihomed AS may re-advertise routes received from one provider AS to the other, thus functioning as a transit AS for its two providers. Such misbehaviour may allow for eavesdropping and may also result in

service disruption. New mechanisms for AS PATH verification appear necessary. Different approaches have been taken by S-BGP, soBGP, and IRV, among other proposals, for addressing security in BGP J. Qiu et al (2007). In this study it is proposed a real-time detection system for ISPs to provide protection against bogus routes. The BGP system has been built based on the implicit trust among individual administrative domains and no countermeasure prevents bogus routes from being injected and propagated through the system. Attackers might exploit bogus routes to gain control of arbitrary address spaces (i.e. prefixes), to either hijack the relevant traffic or launch stealthy attacks. Attackers can directly originate the bogus routes of the prefixes, or even stealthier, further spoof the AS paths of the routes to make them appear to be originated by others. The system learns from the historical BGP routing data the basic routing information objects that assembles BGP routes, and detects the suspicious routes comprised of unseen objects. In particular, this leverages a directed AS-link topology model to detect path spoofing routes that violate import/export routing policies.

Cittadini et al (2008). In this study sufficient condition to guarantee the absence of potentially persistent cycles in the routing is provided. Finally it assess the ability of existing models of policy-based protocols to capture routing cycles, showing that different models put in evidence different types of cycles. Internet Service Providers have at their disposal a powerful policy-based protocol for enforcing a fine grained control of Interdomain routing: the Border Gateway Protocol. However, the price to pay for the flexibility of BGP is the lack of convergence guarantees. In this study of the stability of BGP configurations is done. It tackle the problem of deciding if, given the policy configurations, the routing will converge to a stable state or if there is a potential chance of persistent cycles. It is done with a simple algorithm that relies on new properties of policy-based protocols that are shown to be independent on any specific message timing.

Cittadini et al (2009). This study provides a characterization of safety under filtering, filling the large gap between previously known necessary and sufficient conditions. Border Gateway Protocol allows providers to express complex routing policies preserving high degrees of autonomy. However, unrestricted routing policies can adversely impact routing stability. A key concept to understand the interplay between autonomy and expressiveness on one side, and stability on the other side, is safety under filtering, i.e., guaranteed stability under autonomous usage of route filters. BGP route filters are used to selectively advertise specific routes to specific neighbors. This characterization is based on the absence of a particular kind of dispute wheel, a structure involving circular dependencies among routing preferences. Networks admitting multiple stable states are provably unsafe under filtering, and the troublesome portion of the configuration can be pinpointed starting from the stable states alone. This is especially interesting from an operational point of view since networks with multiple stable states actually happen in practice. Finally, adding filters to an existing configuration may lead to cycles even if the configuration is safe under any link failure.

Dobrescu et al (2009). The problem of scaling software routers is revisited in this study motivated by recent advances in server technology that enable high speed parallel processing—a feature router workloads appear ideally suited to exploit. A software router architecture that parallelizes router functionality both across multiple servers and across multiple cores within a single server. By carefully exploiting parallelism at every opportunity, it is proposed a 35Gbps parallel router prototype; this router capacity can be linearly scaled through the use of additional servers. Prototype router is fully programmable using the familiar Click/Linux environment and is built entirely from off-the-shelf, general-purpose server hardware. The broad implications of this study are twofold: one is that software routers could play a far more significant role than previously believed; the more ambitious extrapolation is that a very different industry structure and way of building networks might actually be within not-so-distant reach.

Fabrikant et al (2008). In this work the concept of sink equilibria is sown as PSPACE complete to analyze and approximate for graphical games. The complexity of a well-known problem in networking by establishing that it is PSPACE-complete to tell whether a system of path preferences in the BGP protocol can lead to oscillatory behavior; one key insight is that the BGP oscillation question is in fact one about Nash dynamics. A new equilibrium concept inspired by game dynamics, unit recall equilibria, which is close to universal and algorithmically promising is proposed. Feamster et al (2005). This study shows routing protocol stability under various conditions. It demonstrate that certain rankings that are commonly used in practice may not ensure routing stability and proves that when providers can set rankings and filters autonomously, guaranteeing that the routing system will converge to a stable path assignment essentially requires ASes to rank routes based on AS-path lengths. Thousands of competing autonomous systems must cooperate with each other to provide global Internet connectivity. Each autonomous system (AS) encodes various economic, business, and performance decisions in its routing policy. The current Interdomain routing system enables each AS to express policy using

rankings that determine how each router in the AS chooses among different routes to a destination, and filters that determine which routes are hidden from each neighboring AS. Because the Internet is composed of many independent, competing networks, the Interdomain routing system should provide autonomy, allowing network operators to set their rankings independently, and to have no constraints on allowed filters.

Gao et al (2001). This study presents a general model for backup routing that increases network reliability while allowing each AS to apply local routing policies that are consistent with the commercial relationships it has with its neighbors. Routing policies are not guaranteed be safe, and may cause protocol divergence. Backup routing is often used to increase the reliability of the network under link and router failures, at the possible expense of safety. In addition, proposed model is inherently safe in the sense that the global system remains safe under any combination of link and router failures. The proof of inherent safety is cast in terms of the stable paths problem, a static formalism that captures the semantics of Interdomain routing policies.

**Corresponding author:**
Reenu Goyal
Research Scholar, Department of Computer Science,
OPJS University, Churu,
Rajasthan (India)
Contact No. +91-8950531842
Email: renu12goel@gmail.com

**References:**

1. A Manjeshwar, DP Agrawal. TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks. Inipdps. 2001; Vol. 1, 189.
2. A Manjeshwar, DP Agrawal. APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. In Ipdps. 2002; Vol. 2, 48.
3. B Chen, K Jamieson, H Balakrishnan, R Morris. Span: An energyefficient coordination algorithm for topology maintenance in ad hoc wireless networks. Wireless networks. 2002; 8(5), 481-94.
4. L Carr-Motyčková, D Dryml. Distributed energy efficient data gathering without aggregation via spanning tree optimization. In International Conference on Ad-Hoc Networks and Wireless. 2013; 87-98.
5. T Qiu, X Liu, L Feng, Y Zhou, K Zheng. An efficient tree-based self-organizing protocol for internet of things. IEEE Access. 2016; 4, 3535-46.
6. A Roshini, H Anandakumar. Hierarchical cost effective leach for heterogeneous wireless sensor networks. In Advanced Computing and Communication Systems. 2015; 1-7.
7. V Sharma, DS Saini. Performance Investigation of Advanced Multi-Hop and Single-Hop Energy Efficient LEACH Protocol with Heterogeneous Nodes in Wireless Sensor Networks. In Advances in Computing and Communication Engineering (ICACCE). 2015; 192-197.
8. AA Malluh, KM Elleithy, Z Qawaqneh, RJ Mstafa, A Alanazi. Emsep: an efficient modified stable election protocol. In American Society for Engineering Education (ASEE Zone 1). 2014; 1-7.
9. T Tiwari, NR Roy. Modified DEEC: A varying power level based clustering technique for WSNs. In Computer and Computational Sciences (ICCCS). 2015; 170-176.
10. BR Al-Kaseem, AO Nyanteh, HS Al-Raweshidy. Self-Organized Clustering technique based on sink mobility in heterogeneous M2M sensor networks. In Students on Applied Engineering (ISCAE). 2016; 431-436.
11. Y Yu, R Govindan, D Estrin. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. Springer. 2001; 211-221.
12. VB Carvalho. 2010, Including context in a routing algorithm for the Internet of Things, Doctoral Dissertation. Faculdade de Ciências e Tecnologia, Lisboa, Portugal.
13. G Di Caro, F Ducatelle, LM Gambardella. Ant Hoc Net: an adaptive nature ‐ inspired algorithm for routing in mobile ad hoc networks. European Transactions on Telecommunications. 2005; 16(5), 443- 55.
14. F Dressler, OB Akan. A survey on bio-inspired networking. Computer Networks. 2010; 54(6), 881-900.
15. M Farooq, GA Di Caro. Routing protocols for next-generation networks inspired by collective behaviors of insect societies: An overview. Springer. 2008; 101-160.
16. IETF, Available at: http://www.ietf.org/ proceedings/82/slides/rtgarea-2.pdf? accessed November 2011.
17. GC Onwubolu, BV Babu. New optimization techniques in engineering. 1st ed. Springer-Verlag Berlin Heidelberg; 2013, p. 1- 2.
18. C Lochert, M Mauve, H Füßler, H Hartenstein. Geographic routing in city scenarios. ACM SIGMOBILE mobile computing and communications review. 2005; 9(1), 69-72.

7/25/2020