Implementation of SPIN Model Checker for Formal Verification of Distance Vector Routing Protocol

Kashif Javed
Department of Information Technologies
Abo Akademi University
Turku, FIN-20520, Finland
Kashif.javed@abo.fi

Asifa Kashif
Department of Electrical Engineering
National University of Computer and
Emerging Sciences, Islamabad, Pakistan
asifa.ilyas85@gmail.com

Elena Troubitsyna
Department of Information Technologies
Abo Akademi University
Turku, FIN-20520, Finland
Elena.Troubitsyna@abo.fi

***Abstract* - Distributed systems and computing requires routing protocols to meet a wide variety of requirements of a large number of users in heterogeneous networks. DVR is one of many other employed protocols for establishing communication using routes with minimum cost to different destinations from a given source. Research work presented in this paper focuses on implementation of DVR in SPIN and provides formal verification of correctness of DVR behaviour covering all required aspects. Simulation results clearly show a proof of the established paths from each router to different destinations in a network consisting of six routers and a number of links.**

Keywords: Formal Verification, DVR Protocol, SPIN Model Checker, Distance Vector Routing, Implementation in PROMELA

I. INTRODUCTION

A computer network consists of a number of routers which have the capability to communicate with each other. Routing Information Protocol (RIP) is widely used for routing packets from a source to its destination in computer networks. RIP requires information about distance and direction from source to destination. Each router, in the Distance Vector Routing (DVR) methodology, keeps updated record of distances and hops of its neighbours. Various techniques are used to gather useful routing table information for each router. In one approach, special packets are sent by each router and are received back after having time-stamped by the receivers. Chromosomes have been employed in the Genetic Algorithm [1] to select the most optimal path by utilizing its fitness function, selection of next generation and crossover operation for updating the routing tables in an efficient manner. Thus, all routers keep refreshing their routing tables and maintain latest information about other neighbouring routers in order to provide optimized performance in the available network [1-3].

Mahlknecht, Madni and Roetzer [4] has presented an efficient protocol that uses hop count and cost information in its Energy Aware Distance Vector (EADV) routing scheme and makes use of shot-multi-hop routing for consuming lesser energy in the wireless sensor networks. EADV can do well for long lasting battery-powered sensor nodes while using the lowest cost path towards the selected sink node. An algorithm is considered the most effective if it contains the correct and latest information about its neighbours in its DVR table. An effort has been made by Liwen He by devising a computational method to protect a network from internal attacks (such as mis-configuration and compromise) through the use of verifying routing messages in the DVR protocols [5]. Formal verification of standards for DVR protocols has also been comprehensively presented by Bhargavan, Gunter and Obradovic [6] using three case studies. The researchers have used HOL (an interactive theorem prover and SPIN (model checker) to verify and prove salient properties of DVR protocols. HOL and SPIN have been employed by these researchers for providing a proof of convergence for the RIP [7].

The remaining paper is organized as follows. DVR protocol is presented in Section II and Section III describes the use of SPIN tool and PROMELA language for formal verification. System design and implementation has been discussed in Section IV covering network topology, implementation details and operation of DVR protocol. Formal verification of simulation results has been illustrated in Section V and finally conclusions and future work is given in Section VII.

II. DISTANCE VECTOR ROUTING PROTOCOL

A. General Methodology

A routing table is required to be maintained for each router in the network for the purpose of working of a DVR scheme. Routing table information is used to determine the best path (i.e. having minimum cost in terms of distance or hops) from a source to destination. Links are needed to connect concerned routers for establishing communication. An optimal DVR protocol has to exchange frequent messages in order to update the routing table of each router. So, exchanging information among neighbours is carried out on regular intervals.

Routing table of every router keeps necessary information (i.e. id of neighbouring routers, most suitable outgoing link to be used for the destination, distance, hops (number of routers on the route), time delay, number of queued messages on the link). The process of making forwarding decision for selecting the best optimal path from source to destination is based on a combination of these parameters. The objective of routers is to send packets to hosts connected to the networks for heterogeneous requirements of a large number of users. In this way, efficient DVR schemes ultimately establish good global

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

paths by connecting hosts in a distributed environment covering very long distances. Those routers are taken as neighbours which have links/interfaces to a common network.

B. Routing Information Protocol

RIP [8,9] is a widely used protocol for finding the optimal path to the destination in a network. Each router has a routing table and all routers periodically updated their routing tables by using advertising approach. All routes of a router are advertised through the mechanism of broadcasting RIP packets to all the neighbouring routers in the network. Every router checks the advertised information of neighbouring nodes and changes information only in its routing table if the new route to the same destination further improves the existing route length. In other words, the updated routing table information now takes to the best available route so far for the relevant destination.

The number of hops in the RIP are kept low (up to 15) for the route length for faster convergence [6,7]. RIP methodology, however, prevents formation of loops between pairs of routers in order to minimize convergence time as well as permitted route length. Timer expiry record is also maintained in every routing table and is normally set to 180 seconds whenever a routing table is updated. As routers advertise after every 30 seconds, the destination is considered unreachable if a router is not refreshed for 180 seconds. It further waits for another 120 seconds. If the router remains un-refreshed during this time as well, then its route is removed from the routing tables of the concerned routers. This requirement is incorporated to cater for broken links, faulty networks and congestions.

III. Use of SPIN and PROMELA

A. Formal Verification

A number of new systems and methodologies are being devised by the researchers in different areas of science, technology and engineering as a result of meaningful R&D work being undertaken by academic and research institutes all over the world. Every proposed system requires a proof of its correctness by gathering results using simulation and testing techniques. Formal verification terminology [10,11] is in fact a process of actual demonstration of the system in order to check its correctness under the defined boundaries and valid conditions of used parameters/variables.

Precision and accuracy of the system is verified by running the programming modules by employing required algorithms in the model checking approach. Errors occurred (if any) are properly identified under varying conditions so that such errors can be easily located by the users and are later on repaired/tackled by adjusting specifications of the model. Afterwards, the model description is fine tuned to achieve required model specifications for verification of correct results of the system.

B. SPIN Tool and PROMELA High Level Language

SPIN [12,13] is a open-source software tool and is widely used for the formal verification of software systems working in the distributed environment. Inspiring applications of SPIN include the verification of the control algorithms for various applications, logic verification of the call processing software for a commercial data communication, critical algorithms for space missions, operating systems, switching systems, distributed & parallel systems and formal verification of various routing protocols. This tool also supports interactive, random and guided simulations for a wide variety of applications. Spin can be used in four main modes (i.e. as a simulator, as an exhaustive verifier, as a proof approximation system and as a driver for swarm verification).

Spin provides efficient software verification and supports the PROMELA (PROcess MEta LAnguage) high level language to specify systems descriptions [14]. It is a SPIN's input language which is used to build detailed PROMELA models for complete verification of system designs. It provides a way for making abstractions of distributed systems. Different assumptions are used in SPIN to verify each model. After checking correctness of a model with SPIN, it can then be used to build and verify subsequent models of the system so that the fully developed system produces the required behavior. PROMELA programs consist of processes, message channels, and variables.

IV. System Design and Implementation

A. Network Topology

The network topology shown in Figure 1 has been used for implementation of DVR protocol. There are six routers (A, B, C, D, E & F) and seven links (edges). Each link connects two routers. Weight values range from 2 to 23 for different links and these values indicate distances between routers. Integer values have been used and distance units can be chosen during actual implementation of the network. For example, the distance between routers A and C via B is 6 using 2 hops and via D, E and F is 33 using 4 hops.

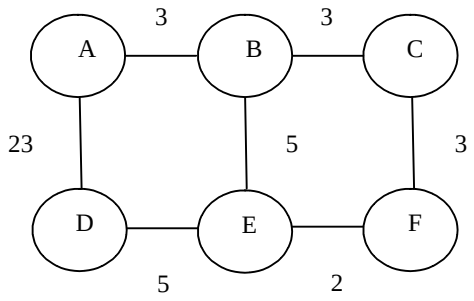

Figure 1: Network Topology

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

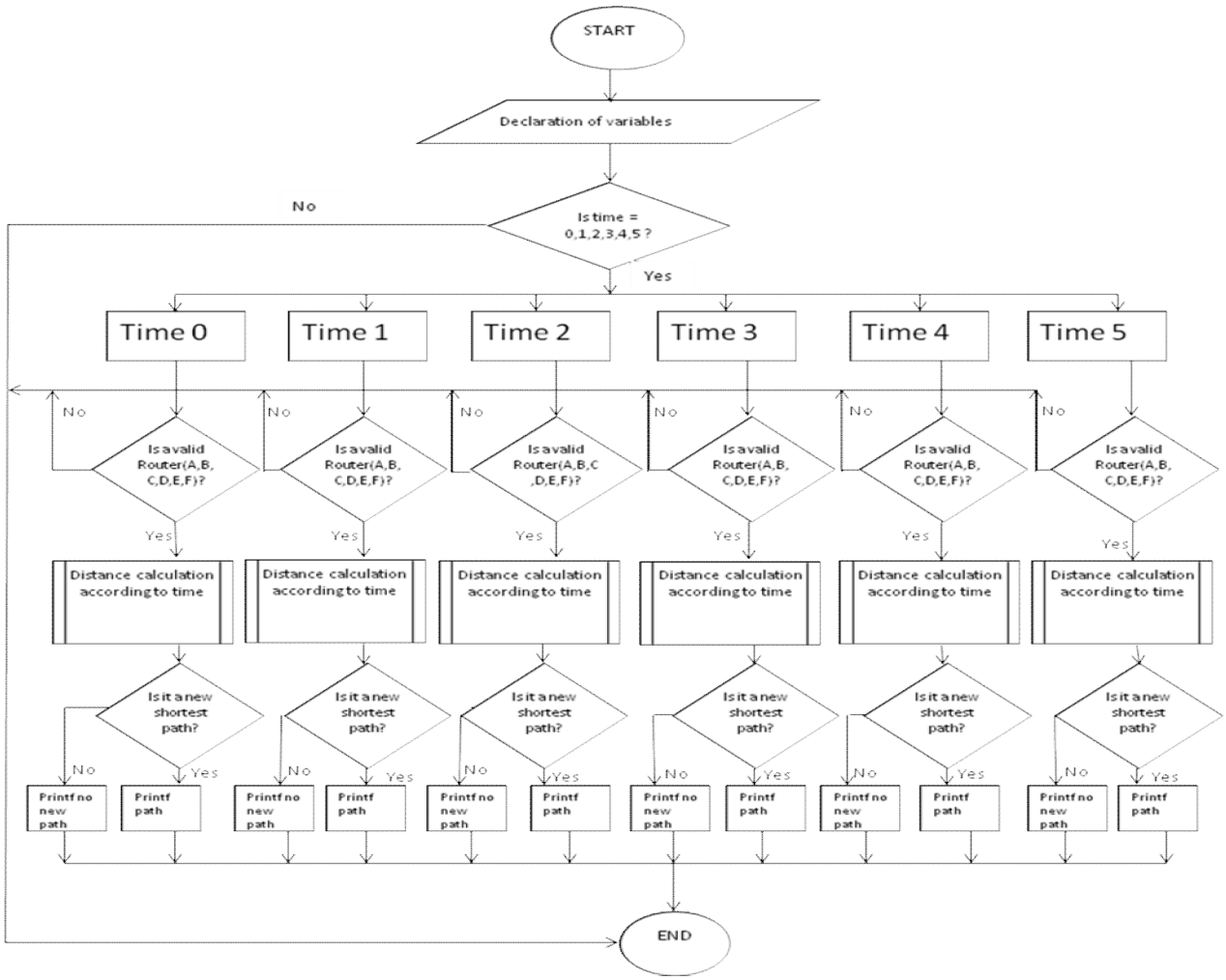

Figure 2: System Flowchart

B. System Implementation

SPIN's PROMELA language has been used to construct complete model of DVR protocol on a Pentium machine. Packets from the source to destination travel using links provided by routers by making use of their routing tables for the given distributed environment of the network. After initialization of the variables, distance is calculated from each router at time period T=0, T=1, T=2, T=3, T=4 and T=5. At each stage it checks whether the measured distance forms a new shortest path or not. Whenever the shortest path is found from the source to destination, routing table entry for the concerned router is automatically updated to make good forwarding decision in order to ensure optimal path, having minimum distance, for faster communication. Thus, each router updates its routing table after each time period. The main objective of the DVR protocol is to provide the current best route (path) from source to destination for each communication. Flowchart of the modeled system in SPIN/PROMELA is shown in Figure 2.

For the given network, the PROMELA program has six processes (one for each time period) to find distance based upon the time period conditions (0 to 5). The found distance from a particular source to destination for each time period is compared with all the available alternate routes. Router's table is only updated if the new distance is minimum between the selected source and destination. The new shortest path is recorded after each calculation. If the determined route does not find minimum distance during the given time period, then it ignores its path without updating any entry in the routing table. Routers improve their routes whenever a router advertises its routing table to its neighbours. So, new routes are determined purely based on their length measured in distance. For timely convergence, the number of hops involved in the length are limited to 15 as already highlighted by Bhargavan et. al. [7].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

		Via							Via							Via					
	From A	A	B	C	D	E	F	From B	A	B	C	D	E	F	From C	A	B	C	D	E	F
T=0	A							A	3						A						
	B		3					B							B		3				
	C							C			3				C						
	D				23			D							D						
	E							E					5		E						
	F							F							F						3
T=1	A							A							A		6				
	B							B							B						
	C		6					C							C						
	D							D	26				10		D						
	E		8		28			E							E		8				5
	F							F			6		7		F						
T=2	A							A					33		A						
	B				33			B							B						10
	C							C					10		C						
	D		13					D							D		13				10
	E							E	31		8				E						
	F		9		30			F							F		10				
T=3	A							A							A		36				13
	B							B							B						
	C		13		33			C							C						
	D							D			13				D						
	E		11					E							E		34				
	F							F	33						F						
T=4	A							A			36				A						
	B				36			B							B						36
	C							C	36						C						
	D		16					D							D						36
	E							E							E						
	F				39			F							F		36				
T=5	A							A							A						
	B							B							B						
	C							C							C						
	D							D							D						
	E							E							E						
	F							F							F						

Table1: Calculated Distance from Routers A, B and C for Different Destinations at Time Periods T=0 to T=5

C. Operation of DVR Protocol

DVR protocol works independently for every destination and it is assumed that there is no topology change for protocol's convergence during every time period. The router broadcasts after every 30 seconds and the destination is taken as inaccessible if it is not refreshed for 180 seconds. The route is removed from the tables of concerned routers if the particular router fails to refresh itself for 300 seconds.

Although the PROMELA's built model can be used for any number of routers but its operation is restricted only to the topology given in Figure 1. For the purpose of explanation of the model, it is assumed that every router operates without any problem and updates its routing table during regular intervals of time.

At Time=0, it calculates distances to neighbouring routers from each router having maximum one hop. Thus, distance from A to B is 3 & A to D is 23from router A; from router B it is 3, 3 & 5 for routers A, C & E respectively; and distances are 5, 5 & 2 for routers B, D & F respectively from router E. These distances can be observed in Tables 1 and 2. Now two hops from the current router are taken for T=1. So, distance from A

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

		Via							Via							Via					
	From D	A	B	C	D	E	F	From E	A	B	C	D	E	F	From F	A	B	C	D	E	F
T=0	A	23						A							A						
	B							B		5					B						
	C							C							C			3			
	D							D				5			D						
	E					5		E							E					2	
	F							F						2	F						
T=1	A							A		8		28			A						
	B	26				10		B							B			6		7	
	C							C		8				5	C						
	D							D							D					7	
	E							E							E						
	F					7		F							F						
T=2	A					13		A							A			9		10	
	B							B				31		8	B						
	C	29				10		C							C					10	
	D							D		31					D						
	E	31						E							E			11			
	F							F		11					F						
T=3	A							A						11	A						
	B					13		B							B					33	
	C							C				34			C						
	D							D							D			16		33	
	E							E							E						
	F	32				16		F							F						
T=4	A					16		A							A			39			
	B							B							B						
	C	36						C							C					36	
	D							D						34	D						
	E	34						E							E			37			
	F							F				37			F						
T=5	A							A							A						
	B							B							B						
	C							C							C						
	D							D							D						
	E							E							E						
	F							F							F						

Table 2: Calculated Distance from Routers D, E and F for Different Destinations at Time Periods T=0 to T=5

to C via B is 6; A to E via D 28; and A to E via B is 8 as given in Table 1.

When T is taken as T=2, three hop lengths are counted for determining the distance from each router. From router D, measured distances are 13 via E to A, 29 via A to C, 10 via E to C and 31 via A to E. Same can be seen in Table 2. Hop length is four when T=3, distance covered to B via E, D via C and D via E is 33, 16 and 33 respectively from router F as shown in Table 2. Similarly, routes have distances of 36 (B via F), 36 (D via F) and 36 (F via B) from router C (for T=4) as given in Table 1. Both Tables 1 and 2 clearly indicate that no routes are available from any router when T=5 (six hops) for network configuration of Figure 1.

V. Formal Verification of Simulation Results

The implemented system in PROMELA programming language has been tested exhaustively and obtained simulation results are shown in Tables 1 and 2. Spin model checker has been used to verify all the results. The developed model ensures that all the routers correctly maintain and update their tables as and when new routes are searched and visited. The broadcast mechanism works well at different time periods and the system provides correct and optimized results from each router to various destinations depending upon network topology, layout of routers and links connecting different routers in the network.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The SPIN's verification model successfully checks all the available routes via different routers and permits only the shortest path from the available options. It is evident from the following decisions (only four out of many are presented here):

1) *At T =1, the route length from E to C via B is 8 where as it is 5 via F. So, E router adopts F router's path to reach C.*
2) *The distance between routers B & E via A and via C is 31 and 8 respectively. SPIN's checker confirms that minimum distance is covered for reaching to C from E when T=2.*
3) *When T=3, the path cost determined by the model is 13 from C to A via F, E & B but another path for connecting the same two router via B, E & D is 36, each path makes use of four hops. Of course, the longer path is simply ignored.*
4) *Similarly, route length from F to D through C, B & A is 32 and it is 16 via routers C, B & E. A saving of 16 is noted while using the most economical path.*

A careful analysis of the simulation results shown in Tables 1 & 2 clearly indicates that the modeled system in PROMELA operates correctly and provides the best possible routes involving minimum distances using DVR protocol on the given network environment. The system works efficiently under all conditions and the SPIN model checker has guaranteed correctness of all results. It means that all the routing tables are timely updated while messages are being sent to various destinations from a particular source. Now, this can be extended to bigger networks in the distributed environment for efficient and correct functioning using SPIN tool.

VI. Conclusions and Future Work

Many researchers have implemented DVR protocols for various applications. In this research work, PROMELA language has been used to implement DVR protocol on a six router model. Formal verification of DVR protocol properties has been shown through the use of SPIN checker model. The simulation results amply demonstrate correctness and reliability of DVR protocol under varying conditions. Performance of the implemented has been extremely well and it can further be improved to make it more efficient in terms of reducing storage space requirements, incorporating security mechanism for safer communication, minimizing congestion at peak loads and making it fault-tolerant for enhancing its reliability and flexibility.

References

[1] M. R. Masillamani, A. V. Suriyakumar, R. Ponnurangam and and G.V.Uma, "Genetic Algorithm for Distance Vector Routing technique", AIML International Conference, 13-15 June 2206, Egypt, pp. 160-163.

[2] Andrew S.Tanenbaum, "Computer Networks", 4th Edition,. Prentice-Hall Inc., 2005.

[3] G. Coulouris, J. Dollimore and T. Kindberg, "Distributed Systems : Concepts and Design, 4th Edition, Addison-Wesley, 2005.

[4] S. Mahlknecht, S. Madani and M. Rötzer, "Energy Aware Distance Vector Routing Scheme for Data Centric Low Power Wireless Sensor Networks," *Proceedings of the IEEE International Conference on Industrial Informatics INDIN 06*, Singapore, 2006.

[5] Liwen He, "A Verified Distance Vector Routing Protocol for Protection of Internet Protocol", Lecture Notes in Computer Science, Networking – ICN 2005, Volume 3421, Springer, pp. 463-470.

[6] K. Bhargavan, D. Obradovic and C. A. Gunter, "Formal Verification of Standards for Distance Vector Routing Protocols", Journal of the ACM, Vol. 49, no. 4, July 2002, pp. 538-576.

[7] K. Bhargavan, C. A. Gunter, and D. Obradovic, "Routing Information Protocol in HOL/SPIN", Proceedings of the 13th International Conference on Theorem Proving in Higher Order Logics 2000, August 14 - 18, 2000, London, UK, pp. 53-72.

[8] C. Hendrick, "Routing Information Protocol", RFC 1058, IETF, June 1988.

[9] G. Malkin, 'RIP Version Carrying Additional Information', IETF RFC 1388, January 1993.

[10] J. Katoen, "Concepts, Algorithms and Tools for Model Checking", Lecture Notes 1998/1999, Chapter1: System Validation.

[11] N. A. S. A. Larc, "What is Formal Methods?", http://shemesh.larc.nasa.gov/fm/fm-what.html, formal methods program.

[12] R. de Renesse and A. H. Aghvami "Formal Verification of Ad-Hoc Routing Protocols using SPIN Model Checker", Proceedings of IEEE MELECON'04, Croatia, May 2004.

[13] G. J. Holzmann, "The Model Checker SPIN", IEEE Transactions on Software Engineering, Vol. 23, No. 5, May 1997, pp. 279-295.

[14] G. J. Holzmann, "Design and Validation of Computer Protocols", Prentice Hall, November 1990.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500