Pertanika J. Sci. & Technol. 27 (3): 1301 - 1316 (2019)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Probabilistic Dempster Shafer based Communication Behaviour Analysis for Attack Safe Communication in Mobile Network

Kapil Juneja

Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, Haryana,124001, India.

ABSTRACT

Security is the primary and integrated requirement for public networks. Internal authenticated attackers are more unfriendly and dangerous to the network. In this paper, a probabilistic Dempster Shafer method is applied to the communication behaviour of network nodes. A prior analytical observation over the communication was done in terms of upper and lower bounds. The upper bound is considered as the belief measure and the lower bound is taken as plausibility factor. The probabilistic belief-to-plausibility measure is obtained for communication delay, failure ratio and energy parameter. As the abnormal activity pair was identified, a verification check was performed before blocking the misbehaving node. The Dempster-Shafer based belief theory was applied to isolate the attacker node and to generate the safe path over reliable nodes. The decision rule was integrated to the work behaviour of the AODV (Ad hoc On-Demand Distance Vector) protocol for the preventive route formation. The simulation results show that the method has improved the communication PDR (Packet Delivery Ratio) ratio and reduced the drop rate and energy consumption as compared to AODV and DSR (Dynamic Source Routing) protocols.

ARTICLE INFO

Article history:
Received: 3 July 2018
Accepted: 27 March 2019
Published: 24 July 2019

E-mail addresses:
kapil.juneja81@gmail.com, kapil.juneja.1981@ieee.org

Keywords: AODV, attack preventive, Dempster Shafer, mobile network, security

INTRODUCTION

The dynamic and cooperative communication in mobile network (Vadlamani et al., 2016;

ISSN: 0128-7680
e-ISSN: 2231-8526

Mavoungou et al., 2016) not only increases the flexibility, but also opens the network to the intruders. The network suffers from different kinds of attacks that acts at access, protocol, communication and architecture level in the mobile network (Mavoungou et al., 2016; Saeed et al., 2014). The network suffers from various internal and external attacks. These attacks affect the network users in terms of integrity, privacy, delayed communication and data disruption. These attacks can infect one or more communication layers and disturb the data transmission. The external attackers are unknown users that enter into the network temporarily and capture the communicating information. These attacks can be avoided by including the network firewall or by using a secure authentication system. But, the internal attacks are comparatively more critical as such attacks are performed by the authenticated users or nodes. These attackers can reveal the information or affect the communication behaviour. To deal with these attackers, the attack detection and prevention algorithms can be applied. The detection algorithms basically observe the attack specific behaviour of mobile nodes. The detection algorithm blocks the identified attacker node and performs the communication. The preventive algorithms also analyze the communication pattern over all nodes and perform the communication through safe nodes. In this paper, a Dempster-Shafer theory based probabilistic model is presented to generate the safe communication route over the mobile network. The preventive algorithm used the multiple decision factors such as communication delay, failure ratio and node energy. The belief and plausibility factors are generated under Dempster Shafer based node verification model. The abnormal activity based on these parameters are analyzed to recognize the misbehaving node and to generate the safe preventive path over the network.

Dempster Shafer

It is the dynamic generalization of Bayesian Probabilistic evaluation. The Bayesian theory can be applied as a divergence factor to recognize the communication pattern and to isolate the normal and misbehaving nodes. To validate a node, the confidence factor based on multiple communication factors can be analyzed. In these methods, the conditional evaluations are applied in a controlled way to derive the decision. These factors are analyzed individually as well as in composite form to take the decision. To apply the Dempster Shafer (Elkin et al., 2017; Karami & Fathian, 2009; Konorski & Orlikowski, 2009; Wahab et al., 2014; Zhang et al., 2017) theory, the probabilistic decisions are computed as the belief variable. Let n is the number of probabilistic factors and $Eval$ () is the function to perform the probabilistic computation on each factor. The aggregative belief theory for all factors is represented as equation (1)

$$\sum_{i=1}^{n} Eval(V_i) \quad =1 \qquad (1)$$

Here, V represents the parameters analyzed to take the composite decision. These

parameters are also controlled by the specification of upper bound, lower bound and the degree of confidence. The value of confidence degree μ lies between 0 and 1.

This DS (Dampster Shafer) theory is described by two main aggregative functions called Belief and Plausibility. The Belief shown in equation (2) represents the upper bound and the plausibility shown in equation (3) represents the lower bound of probability

$$\text{Belief(B)} = \sum_{V_i \subset B} Eval(V_i) \qquad (2)$$

and

$$\text{Plausibility(B)} = \sum_{V_i \cap B = \emptyset} Eval(V_i) \qquad (3)$$

Where, Eval is the evaluating function on which the aggregative measures are applied to take the probabilistic composite decision.

Problem Definition

The mobile network is the public network in which multi-hop communication is performed in the absence of any controller device. The attacker can infect any of the intermediate nodes at different layer. In this paper, the problem of man-in-middle attack is addressed at the network layer of mobile network. The attack is accomplished by the attacker to disturb the packet delivery by avoiding the data forwarding or increasing the delay. As the attack is performed on the existing contributing node, it is difficult to attack. The communication-level observation is the only way to analyze the behaviour of the nodes and to detect the attack. This paper has presented a solution against the man-in-middle attack. The contributions of this paper to optimize the network performance against man-in-middle attack are listed below:

- The paper presents a dempster-shaper theory based probabilistic analysis approach for evaluating the reputation of nodes.
- The proposed reputation-based method has isolated the attacker nodes and generates a attacker-preventive route for improving the reliability of communication in public mobile network.
- The work is defined as modified-AODV protocol for enabling a attack-safe communication in mobile network.

In this paper, a Dempster Shafer based probabilistic evaluation method is integrated to improve the intelligence of traditional AODV protocol. Multiple parameters are evaluated to identify the weights for mobile nodes and to identify the possible route contributing nodes. The proposed PDS-AODV (Probabilistic Dempster Shafer-Ad hoc On-Demand Distance Vector) protocol is able to generate the attack preventive safe route for mobile network. In this section, brief introduction to the security flaws exist in the mobile network

is discussed. The exploration of the Dempster Shafer theory is also provided in this section. In section "Related Work", the contributions of earlier researchers are discussed to explore the network challenges and to detect and prevent the attacks over the mobile network. In section "Method", the functional stages of proposed Dempster Shafer based intelligent PDS-AODV protocol are described with algorithmic formulation. In section "Results and Discussion", the simulation results obtained from different scenarios are presented in graphical form. In section "Conclusion", the conclusion and future scope of this work are provided.

RELATED WORK

The cooperative communication in wireless network and lack of centralized infrastructural control enables the open and instant connectivity to a user (Vadlamani et al., 2016). This open and flexible communication mechanism increases the chances of data theft and communication disruption. The security of the network gets compromised because of the different kind of internal and external attacks (Mavoungou et al., 2016). Various authentication, detection and prevention based methods were recommended by different researchers to increase network effectiveness against specific attacks. Different node level and network level attacks can affect the behaviour of different network layers. In this section, contribution of earlier researchers for identification of various attack detection and safe communication methods is provided. Different network layer attacks and its effect on AODV protocol was identified by (Saeed et al., 2014). A detailed description of different anomaly detection techniques including classification, clustering and statistical methods were provided by (Ahmed et al., 2016). Author processed the work on different communication data repositories and evaluates different detection methods against different types of attacks. A study on intrusion detection frameworks was provided for safe communication in wireless networks (Brutch & Ko, 2003). An analytical derivation of different attack preventive methods in AODV protocol was provided based on different communication phenomenon (Hassan & Radenkovic, 2014).

To locate the collaborative attacks and to provide the safe communication in mobile network, the dynamic communication behaviour methods and protocols were suggested by different researchers. Rana et al. (2015) had proposed and enhanced modified AODV protocol to provide communication over reliable nodes. The hop restriction based reverse path tracing was computed by the author for generation of safe route between source and destination. An attack preventive behaviour was integrated in OLSR (Optimized Link State Routing) protocol by generating the periodic validation messages (Abdalla et al., 2011). The neighbour verification process was defined to evaluate the attacker ranking. An intelligent game theoretic framework was proposed to generate the secure multipath route by observing the communication features (Sarkar & Datta, 2017). The minimax probabilistic learning

was defined to increase the bandwidth utilization, PDR and to reduce the routing overheads. Sathiamoorthy and Ramakrishnan (2017) had proposed a competent Three Fish algorithm for effective tracking of neighbour nodes and to provide the effective route discovery. The unique key based trust evaluation method was defined for attaining the safe route in mobile networks. Taheri et al. (2015) had proposed an anonymous multicast routing protocol with additional privacy features for secure communication in mobile networks. The routing protocol was applied on dynamic topology based network to optimize network maintenance and data forwarding mechanisms. A probabilistic proactive routing method with hint extensive control was proposed for effective route selection (Nejad et al., 2010). The hint computation was obtained based on time and packet hint factorss. The distance based correlation is also established to identify the gossips and the false communication between node pairs.

Thanigaivel et al. (2012) had performed optimal route discovery based on node trust evaluation. The cooperative communication was measured to ensure the trust between node pairs and to isolate the malicious node. Author considered the characterization of various attacks to decide the node trust. An integrated mathematical model based on node reliability and residual energy was designed to generate the stable and safe route (Xing et al., 2009). The weight driven joint formula was defined to characterize the node credibility.

METHOD

Mobile public network is always under the threat of various attacks performed by internal nodes. In this paper, a probabilistic Dempster Shafer theory based analytical model is presented to analyze the abnormal behaviour of neighbour nodes. To adapt the analytical observations relative to aggregative communication statistics, the upper and lower limits were obtained. The Dempster-belief modeling was applied at this stage to apply the plausibility and belief measures. The node strength evaluation was done based on communication delay, failure ratio and energy parameters. At the earlier stage, the clear abnormal nodes were separated and the deep evaluation was performed on the eligible contributing nodes. At the final stage, the verification check was applied to identify the safe neighbour. This process is applied as the integration to AODV protocol and accomplished while locating the effective next hop. The functional stage driven model associated with this work is shown in Figure 1.

Figure 1 shows the functional connectivity derivation of the network under probabilistic belief theory. These functional stages are integrated into the traditional AODV protocol as the integrated work stages. With each work stage, the node level evaluation and rule filtration are performed on collected communication statistics. To initiate the functional process, the mobile network is defined in the wide geographical area. The mobile nodes with energy specification are deployed at random position. The communication coverage and

the sensing strength are defined as the network constraints. To perform the communication, the source and destination nodes are defined as the node pair for which the communication is established. Each of the associated functional stages and the algorithmic behaviour of Dempster-Shafer probabilistic evaluation process is described hereunder:

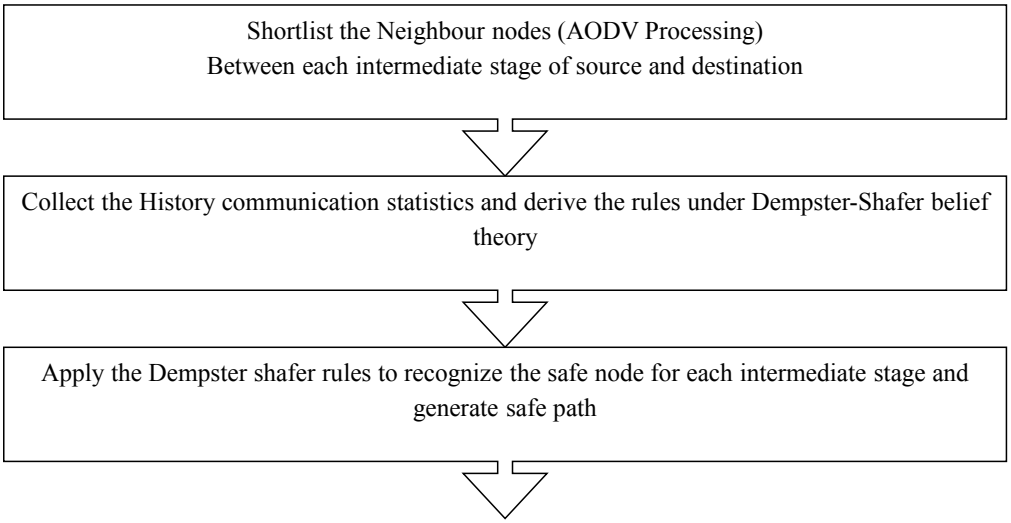


Figure 1. Functional Stages of Attack Safe Communication in Mobile Network

Neighbour Evaluation

As the communication established between the node pair, the AODV protocol is activated at the network layer to perform the early neighbour discovery. The neighbour discovery process initiated from source node and generated the RREQ (Route Request) flooding on the neighbour nodes present in the coverage. This AODV based flooding was spreaded among the neighbour nodes within the expanding ring till the destination does not reach. The neighbours located for each node are maintained in tabular form. At the earlier level the basic node features are evaluated to shortlist the neighbour list ad effective contributing nodes. The node level evaluation is done on node energy and degree factor to perform the parameter selection. The primary level evaluation of node eligibility is shown in the algorithm 1.

Algorithm 1
PrimaryNodeEligibilityEvaluation

Input : Cnode : is the next possible effective hop
Output : EligibilityLevel : between 0 and 3 to represent the strength of node
Process :
1. pNode=GetPrevHop(Cnode) /*Get last selected hop*/

2. degree = GetDegree (Cnode, AODVCover) /*Get sensing range and coverage based degree of node*/
3. nnodes = GetNeighbours(pNode) /*Get all alternate nodes for current level*/
4. AvgEnergy=EvalEnergyState(nnodes) /*Get Average energy of nodes present at that level*/
5. AvgDegree=EvalDegree (nnodes) /*Get Average Degree of nodes present at that level*/
6. If (Cnode.Energy>=AvgEnergy And degree>AvgDegree)
   Then
      Eligibility Level=3
   Else If(Cnode.Energy>=AvgEnergy or degree> AvgDegree)
Then
   Eligibility Level=2
Else If(Cnode.Energy>=AvgEnergy-Limit1)
Then
   Eligibility Level=1
ElseIf(degree> AvgDegree-Limit2)
Then
   Eligibility Level=1
Else
   Eligibility Level=0
End
Return Eligibility Level

Algorithm 1 has defined the identification of next possible effective hop based on node constraint evaluation. The node strength is measured based on energy and node degree parameters. Multiple composite conditions are defined to estimate the strength of the node. The node strength values are between 0 and 3. The nodes with zero strength are unsafe or critical nodes. The node with strength 3 are high featured node to generate optimize safe route between the source and destination nodes. The nodes with higher energy and with multiple connectivity range are considered as safe node. The eligibility level 1 is based on the limit1 and limit2 factors which are decided by the environmental evaluation. These nodes can be considered as part of the communicating path if no alternate exits. After this primary evaluation stage, the effectively eligible nodes are identified.

Dempster-Shafer Rule Formulation

To measure the communication effectiveness and node trust, the dynamic parameter based reputation estimation was done. Dempster-Shafer based evidential and probabilistic rules

were formed to determine the composite reputation for each node. These rules were formed based on the communication history evaluation for specific sessions. The rules were formed to isolate the suspicious and good communication node in previous and random sessions. The history based statistics are collected based on the communication characteristics on M previous random sessions. The communication statistics are collected in terms of average communication delay, PDR ratio, forwarder count and energy consumption parameters. These aggregative and average statistical measures are considered as the evidence for generation of reputation rules. Each of these parameters is evaluated on average communication of m random sessions. Let A is the average statistical feature, then its probabilistic evaluation is given by Measure(A). The compositional evaluation on two communication measures is shown in equation (4)

$$Comp(A,B) = \frac{\sum_{A \cap B} Measure(A) Measure(B)}{1-k} \qquad (4)$$

Each of the individual communication evaluation feature was analyzed in compositional average and aggregative evidential rules. In equation (4), the average feature is represented by A and the aggregative evidential feature is represented by B. The compositional evaluation Comp(A,B) is evaluated for each of the communication parameter for each node. These collective uncertainty observation constraints are able to isolate the healthy and the suspected nodes. The threshold limits are applied separately on each measure by training the network respective to different threshold values. The most significant threshold RTh_{PDR}, RTh_{delay}, RTh_{En} are evaluated to generate the reputation rules. A simulation on 100 and 1000 seconds was conducted on 100 and 200 nodes network with reputation threshold(RTh) values for each uncertainty evaluation parameter. The simulation scenarios are designed with 10% of attacker nodes distributed randomly over the network. The decisive readings collected from the simulations for each parameter are listed in Table 1.

Table 1

Reputation Threshold Evaluation for Different Uncertainty Factors

$RTh_{PDR,\ RThdelay,\ RThEn}$	Sim 1(100 Sec, 100Nodes)	Sim 2(100 Sec, 200Nodes)	Sim 3(1000 Sec, 100Nodes)	Sim 4(1000 Sec, 200Nodes)
(.5,.5,.5)	0.3	0.4	0.48	0.52
(.5,.5,.4)	0.3	0.5	0.46	0.5
(.6,.5,.4)	0.4	0.4	0.45	0.51
(.6,.4,.4)	0.4	0.6	0.5	0.56
(.7,.4,.4)	0.5	0.6	0.56	0.62
(.7,.4,.3)	0.6	0.8	0.59	0.67
(.7,.3,.3)	0.7	0.8	0.67	0.78

Table 1 *(Continued)*

$RTh_{PDR,\ RThdelay,\ RThEn}$	Sim 1(100 Sec, 100Nodes)	Sim 2(100 Sec, 200Nodes)	Sim 3(1000 Sec, 100Nodes)	Sim 4(1000 Sec, 200Nodes)
(.8,.3,.2)	0.8	0.7	0.79	0.88
(.8,.2,.2)	0.8	0.9	0.83	0.91
(.8,.2,.2)	0.9	0.9	0.86	0.93
(.9,.2,.2)	0.6	0.8	0.71	0.74
(.85,.2,.2)	0.9	1	0.88	0.96
(.85,.2,.15)	0.7	0.9	0.81	0.87
(.85,.15,.15)	0.6	0.8	0.71	0.74

Table 1 showing the observations conducted on four different simulations with node and simulation time variations. Different values of reputation thresholds are applied for each uncertainty factor. The evaluation is done in terms of the association of attacker nodes corresponding to each mobile-node. The table shows that the reputation threshold combination (.5,.5,.5) has given the minimum attack detection rate of .3 to .5. As the RTh_{PDR} ratio is increased and the RTh_{delay} and RTh_{En} values are increased, the attack detection rate is improved. The maximum attack detection ratio is obtained for reputation threshold values (.85,.2,.2). These values are considered as final value while generating the safe route in proposed PDS-AODV protocol. Likewise, the uncertainty parameter based evaluation is performed on node-pairs to isolate the safe and attacker nodes. The functional contribution was analyzed based on these reputation parameters and the expected attackers are identified over the network. After identification of attacker nodes, the preventive safe path is generated to ensure the higher PDR ratio. The safe path formulation method integrated in proposed PDS-AODV protocol is described in "Safe Route Generation".

Safe Route Generation

After inspecting the behaviour, the reputation value of each node and node-pair is identified. These reputation values have labeled the nodes as safenode, suspected node and the attacker node. The proposed PDS-AODV protocol evaluated these reputation values at the earlier stage before allowing the real communication. As the communication between a node pair is initiated, the dynamic preventive path is generated. In this path, the neighbour node discovery is evaluated based on the reputation and belief theory aspects. The attacker reputation nodes are completely neglected while generating the route. The suspected nodes can be considered as an intermediate node by performing the dual evaluation and observing the requirement of the network. If the network load is high and the degree of immediate neighbour is low, the suspected node can be considered as an intermediate node for a session. The evaluation of the nodes and traffic is done session by session and with

each session, the new path can be generated. The protocol has generated the on-demand dynamic path with the higher safety and reliability. The algorithm for route generation between a node pair is presented in algorithm 2.

Algorithm 2

SafeRouteGeneration

Input : SNode : SourceNode
DNode : DestinationNode
MNodes : Mobile Nodes

Output : SRoute : The Dynamic Path generated for the current session

Process :

1. CNode=SNode /*Set Source Node as Current Node*/
2. While CNode <> DNode /*Repeat the process for */
Begin
3. Neighs=GetNeighours(CNode, Range) /*Get the Neighbour Node*/
4. Neighs.Stability=AnalyzeStability(Neighs, Session) /*Analyze the node mobility over the session and identify the stability status of neighbour nodes*/
5. ASta=Average(Neighs.Stability)
6. ForEach node in Neighs /*Process the Neighbour Nodes*/
Begin
7. If (node.Stability > ASta) /*A Highly stable node is considered as possible next hop */
Then
8. Eval=PrimaryNodeEligibilityEvaluation(node) /*Perform earlier evaluation based on degree and energy parameters defined in Algorithm 1*/
9. If (Eval=1) /*First level eligibility of node is verified*/
10. RepScore=CalculateReputation (node) /*Estimate the session specific reputation of nodes based on energy, load, PDR and delay parameter as defined in section "Dempster-Shafer Rule Formulation"*/
11. CNode= Max || RepScore ⊗ node.Stability ⊗ Eval || /*Identify most adaptive next neighbour*/
12. SRoute.Add (CNode) /*Include the node in path*/
End If
End If
End If

End
Return SRoute
End

Algorithm 2 has provided the integrated functioning of proposed PDS-AODV protocol to generate the attack preventive safe path in mobile networks. The protocol improved the existing on-demand route formation based on primary and Dempster Shafer evaluation. After specification of source and destination nodes, three level checks are performed to generate the safe route between the node pair. At the earlier level, the coverage range and stability analysis are done to generate the primary neighbour list. In the second stage, the energy, load and neighbour degree evaluation is done to shortlist the effective node. At third level, the Dempster Shafer model is applied to analyze the communication characteristics for the particular session. The communication feature level plausibility and reputation is evaluated at this stage. The feature specific reputation is computed for each expected neighbour. Once the aggregative and average statistics on communication parameters is obtained, the composite evaluation on reputation is done based on the adaptive reputation thresholds. The uncertainty features classified the nodes as safe node, suspected node and attacker nodes. Finally, during the route formulation the factors of all three stages are applied compositely to identify the node with maximum strength or weight. This process is applied on each hop till the destination node does not occur. The model identifies a reliable and safe mode. The functional behaviour of the route formulation method is also shown in Figure 2.

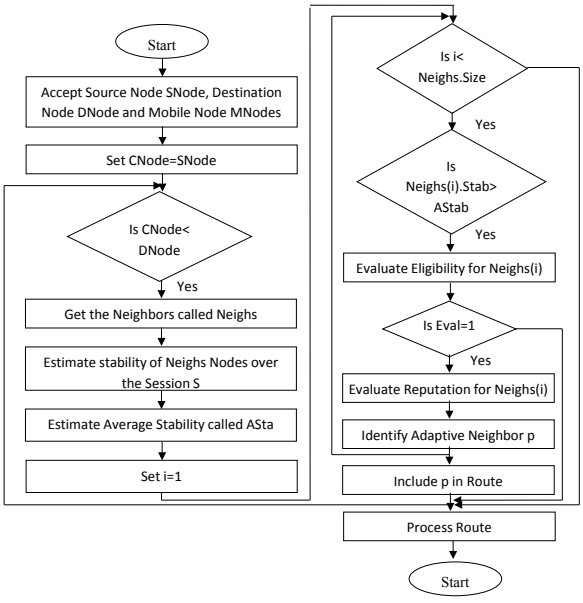


Figure 2. Functional flow of preventive route formation

The figure has provided the process flow for generating the route between any pair of source and destination node. Each time, the effective neighbour is generated by evaluating the stability and reputation of nodes. The most adaptive and effective node is selected as the next communication hop. The method is effective to generate the preventive route over the network. The simulation results with comparative evaluation are provided in the next section.

RESULTS AND DISCUSSION

In this paper, probabilistic rule adaptive belief theory is applied on individual node under node features and communication features. The composite history based evaluation is performed on multiple sessions to isolate the valid safe nodes and the unsafe nodes. The proposed method is able to generate the safe communication route over the network. The proposed method is integrated into the existing AODV protocol to enhance the discovery of safe neighbour and the route. The simulation of the proposed predictive routing protocol is done in NS2 environment on a random mobile network with 100 mobile nodes. The network configuration parameters are listed in Table 2.

Table 2
Configuration Parameters

Parameters	Values
Network Size	1000x1000 Mtr
MAC Protocol	802.15.4
Routing Protocol	AODV, DSR and PDS-AODV
Number of Nodes	100
Number of Attacker Node	0, 2, 5, 10, 20
Node Energy	Random (0 to 1 J)
Energy Consumption (Receiver Node)	5 nJ
Energy Consumption (Transmitter Node)	5 nJ
Energy Consumption (Forwarder Node)	1 nJ
Topology	Random
Mobility	Low

The proposed probabilistic belief improved AODV protocol is able to provide the safe communication against different attacks. As the number of attackers in a network increases, the communication loss and communication delay increases. The evaluation of the proposed protocol is done in terms of drop rate, PDR ratio and energy consumption parameters. The observations are collected for different number of attackers in the network. The comparative results are taken against the AODV and DSR protocols.

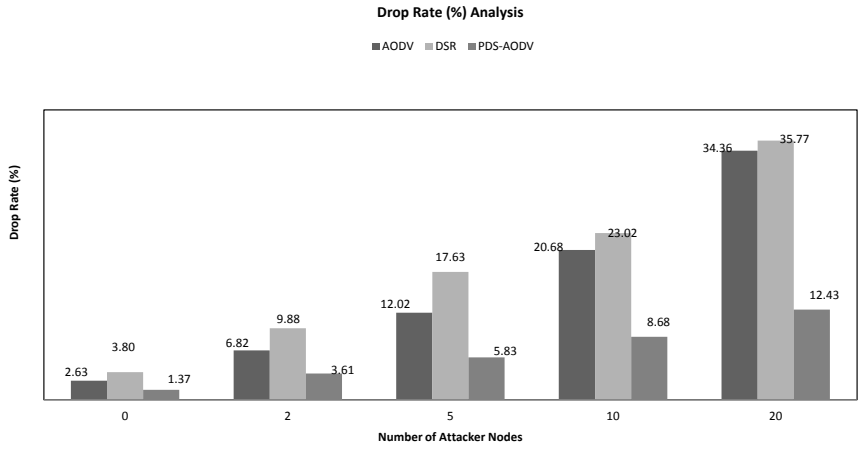
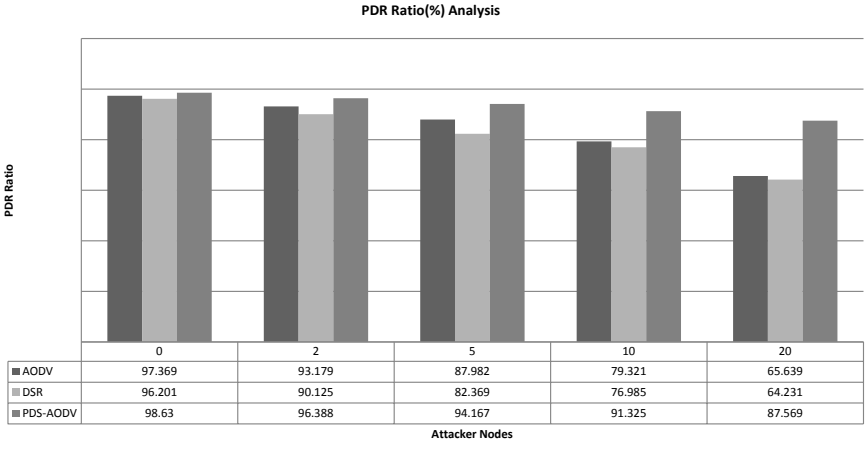


Figure 3. Drop Rate Vs. Attacker Node

When the communication is performed over the attacker nodes, the data loss occurs. The average number of communication loss over all sessions is identified as drop rate. The higher the drop rate compromises the reliability of communication network. Figure 3 shows the comparative analysis of the PDS - AODV protocol against AODV and DSR protocols for different number of attackers. The evaluation results show that the drop rate is increasing in a higher ratio in case of AODV and DSR protocols as the number of attackers increased. The maximum drop ratio in case of the proposed protocol is 12.4%, whereas the drop ratio was over 30% for AODV and DSR protocols. The simulation results signify that the PDS-AODV discovered the safe path by preventing the attacker nodes.



	0	2	5	10	20
AODV	97.369	93.179	87.982	79.321	65.639
DSR	96.201	90.125	82.369	76.985	64.231
PDS-AODV	98.63	96.388	94.167	91.325	87.569

Figure 4. PDR Ratio Vs. Attacker Node

PDR ratio identifies the average number of packets delivered successfully within the specific time limit. The communication performed over attacker nodes, reduces the packet delivery ratio. If the communication is performed over normal and healthy nodes, the higher PDR ratio can be achieved. The proposed PDS-AODV protocol has generated the path using normal safe nodes. The comparative observations are shown in figure 4 on different number of attackers. The evaluation results show that the proposed protocol has increased the PDR ratio extensively. As the attacker nodes are increased, the PDR ratio is dropped up to 64.2%, whereas in case of the PDS - AODV protocol, the PDR ratio is comparatively high upto 87.57%.

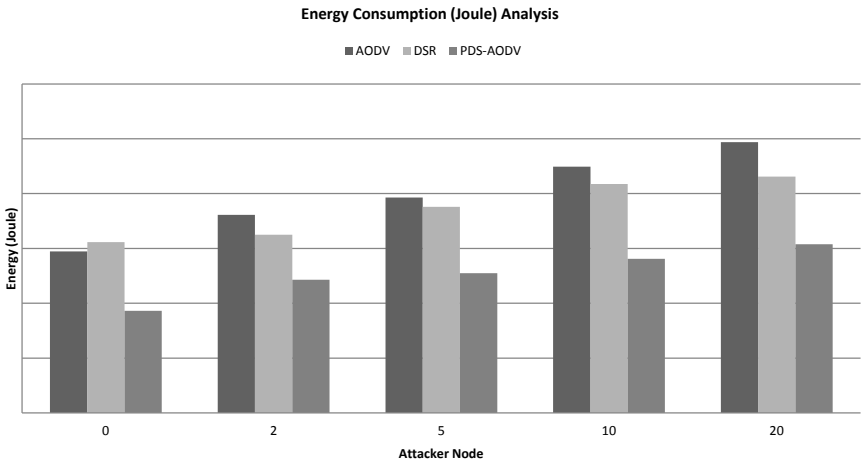


Figure 5. Energy consumption analysis

The primary strength parameter for a mobile node is energy that represents the health of the node. As a node participates in the communication as sender, receiver or forwarder, some amount of energy is consumed. The aggregative energy of all nodes of network represents the network life. The higher the energy consumption in a network, more critical the network will be for further communication. Figure 5 shows the comparative analysis of proposed PDS-AODV protocol against AODV and DSR protocols in terms of energy consumptions. The recorded observations show that the proposed protocol has reduced the energy consumption and improved the network reliability.

CONCLUSION

The paper has presented the belief theory based routing protocol to identify the suspicious behaviour of mobile nodes and to generate the safe route over the mobile network. The work is presented as an improved PDS-AODV protocol in which the work is divided in three sequential work stages. At each stage, the belief and plausibility checks are performed to

generate the reputation weights of mobile nodes and to isolate the safe and attacker nodes. The probabilistic belief theory is implied on energy, delay and PDR ratio parameters and compared with reputation thresholds to identify the expected safe nodes. In the final stage, the maximum reliability constraints on session parameters are applied to identify the next effective hop. The proposed protocol is simulated in NS2 environment and comparative evaluation is taken against AODV and DSR protocols. The analytical results identified that the model has significantly improved the PDR ratio and reduced the drop rate and energy consumption over the network.

ACKNOWLEDGEMENT

The authors have no any conflict of interest or any institution related to this manuscript. I would like to thanks my family members for their support and appreciation.

REFERENCES

Abdalla, A. M., Saroit, I. A., Kotb, A., & Afsari, A. H. (2011). Misbehavior nodes detection and isolation for MANETs OLSR protocol. *Procedia Computer Science, 3*, 115-121.

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19-31.

Brutch, P., & Ko, C. (2003, January 27-31). Challenges in intrusion detection for wireless ad-hoc networks. In *Proceedings of 2003 Symposium on Applications and the Internet Workshops* (pp. 368-373). Orlando, USA.

Elkin, C., Kumarasiri, R., Rawat, D. B., & Devabhaktuni, V. (2017). Localization in wireless sensor networks: A Dempster-Shafer evidence theoretical approach. *Ad Hoc Networks, 54*, 30-41.

Hassan, A., & Radenkovic, M. (2014, August 13-15). Simulation of security attacks and preventions on AODV protocol in ns-3. In *Fourth edition of the International Conference on the Innovative Computing Technology (INTECH 2014)* (pp. 158-163). Luton, UK.

Karami, M., & Fathian, M. (2009, November 9-12). A robust trust establishment framework using Dempster-Shafer theory for MANETs. In *International Conference for Internet Technology and Secured Transactions, (ICITST)* (pp. 1-7). London, UK.

Konorski, J., & Orlikowski, R. (2009, December 20-23). Data-Centric Dempster-Shafer Theory-Based Selfishness Thwarting via Trust Evaluation in MANETs and WSNs. In *3rd International Conference on New Technologies, Mobility and Security* (pp. 1-5). Cairo, Egypt.

Mavoungou, S., Kaddoum, G., Taha, M., & Matar, G. (2016). Survey on threats and attacks on mobile networks. *IEEE Access, 4*, 4543-4572.

Nejad, K. K., Ahmed, S., Jiang, X., & Horiguchi, S. (2010). Probabilistic proactive routing with active route trace-back for MANETs. *Ad Hoc Networks, 8*(6), 640-653.

Rana, A., Rana, V., & Gupta, S. (2015). EMAODV: Technique to prevent collaborative attacks in MANETs. *Procedia Computer Science, 70*, 137-145.

Saeed, A., Raza, A., & Abbas, H. (2014, June30 - July 2). A survey on network layer attacks and AODV defense in mobile ad hoc networks. *IEEE Eighth International Conference on Software Security and Reliability-Companion* (pp. 185-191). San Francisco, CA, USA.

Sarkar, S., & Datta, R. (2017). A game theoretic framework for stochastic multipath routing in self-organized MANETs. *Pervasive and Mobile Computing, 39*, 117-134.

Sathiamoorthy, J., & Ramakrishnan, B. (2017). Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs. *Journal of Information Security and Applications, 36*, 43-58.

Taheri, S., Hartung, S., & Hogrefe, D. (2015). Anonymous group-based routing in MANETs. *Journal of Information Security and Applications, 22*, 87-98.

Thanigaivel, G., Kumar, N. A., & Yogesh, P. (2012, May 16-18). TRUNCMAN: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network. In *2012 Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP)* (pp. 261-266). Bangkok, Thailand.

Vadlamani, S., Eksioglu, B., Medal, H., & Nandi, A. (2016). Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics, 172*, 76-94.

Wahab, O. A., Otrok, H., & Mourad, A. (2014). A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles. *Computer Communications, 41*, 43-54.

Xing, J., Li, Y., Yang, Q., & Shi, H. (2009, September 24-26). A Reliable Routing Model Based on the Residual Energy in MANET. In *5th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-4). Beijing, China.

Zhang, L., Ding, L., Wu, X., & Skibniewski, M. J. (2017). An improved Dempster–Shafer approach to construction safety risk perception. *Knowledge-Based Systems, 132*, 30-46.