SOCIAL PLATFORM BROADCAST SCHEME FOR WIRELESS SENSOR NETWORKS BASED ON SECURITY SYSTEMS

[1]N.Prasanth Kumar, [2]G.Shivakrishna, [3]Ch.Venkanna, [4]Doddolla Praveena
[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Computer Science Engineering, Brilliant Grammar School Educational Society Group of Institutions Integrated Campus, Hyderabad, India

ABSTRACT

In flexible spontaneous organizations, the overhead caused by broadcast plans cannot be disregarded. It is understood that the probabilistic transmission plot, in which hubs transfer parcels with likelihood to reduce excess retransmissions, is a potent technique to cope with reducing overhead. In dangerous situations, toxic hubs degrade network performance; as a result, they should be prevented from course disclosure and information transfer. In this case, the extra steering packages sent by poisonous hubs. This study offers a Trust-based Probabilistic Broadcast scheme (TPB) that focuses on declining overhead, primarily caused by harmful hubs, and in which rebroadcast is not inflexibly dependent on the dependability of hubs. A light-weight trust the executive's methodology is designed based on direct and recommended trust proof to determine hubs' trust level. As indicated by hubs' trust level, rebroadcast delay is determined for revamping the rebroadcast request of steering bundles. Moreover, a clever strategy dependent on hubs' reliability is proposed to compute rebroadcast likelihood, which forestalls entrusted hubs from course revelation. The proposed trust based probabilistic transmission conspires is joined with existing steering convention and its exhibition is assessed by recreations. The mathematical outcomes show that the proposedplan can get network correspondence and diminish the directing overhead.

INTRODUCTION

A mobile assembly network (MANET) is a decentralized remote organization made up of a few movable hubs all of a sudden. MANET-based applications are becoming more and more in demand in a wide range of civilian and military fields, from providing crisis communications in catastrophic events to disseminating basic information on the front lines. These applications are made possible by characteristics like simple organization, dynamic geography, self-setup, and multi-bounce correspondence. Nevertheless, because to resource limits in terms of distant asset and computing power, the MANET presentation is defenseless against directed overhead Moreover, because there is no established entity in charge of management, MANET is defenseless to attacks by vengeful hubs [1], [2]. As a result, it is essential to reduce these risks in order to strengthen the company. The transmission plot is a scattering procedure, wherein hubs convey data to their neighbors [3], [4]. It is extremely normal in MANET steering conventions [5], [6] to scatter directing bundles like Route REQuest (RREQ). The fundamental activity of broadcasting is not difficult to execute by permitting hubs to rebroadcast all approaching directing bundles however make a lot of excess parcel and burn-through such a large number of assets as far as remote data transfer capacity and transmission power. This peculiarity is named communicated storm issue [7], which is a danger to the organization execution. Probabilistic transmission [8] is one of the transmission plans to ease broadcast storm issue, in which hubs rebroadcast bundles as indicated by a predefined likelihood to lessen excess sending. The likelihood can be a fixed value not really set in stone dependent on neighborhood or worldwide boundaries, for example, hubs thickness, versatility level, outstanding energy, distance, and so on [4], [9]. Nonetheless, this multitude of plans don't think about the dependability of hubs [10]. For this situation, assuming hubs make trouble anddon't collaborate to advance parcels dependent on the predefined likelihood, the die out issue [11] canhabitually happen. Then again, these vindictive hubs might harm network associations by dispatching different assaults [12]. In the event that courses contain malignant hubs, the organization execution will be corrupted. Thusly, it is fundamental to think about the reliability of hubs in course disclosure. The RREQ parcel is generally utilized in course disclosure. Truth be told, the course is dependably the one proliferation way of the RREQ bundle from the source to the objective. Since vindictive hubs corrupt theorganization proficiency, they ought to be kept from course revelation and information transmission. For thissituation, directing parcels sent by vindictive hubs are excess. To diminish the overhead, particularly brought about by vindictive hubs in MANET, we propose aclever Trustbased Probabilistic Broadcast plot (TPB), which accepts hubs' reliability as a

critical component to ascertain rebroadcast likelihood. Hubs with lower trust level have a lower likelihood in course disclosure. TPB conspire has the accompanying advantages: 1) The trust-based probabilistic transmission plot diminishes the quantity of excess rebroadcasting bundles brought about by pernicious hubs, so that comparing remote correspondence assets are delivered for information transmission; 2) The likelihood of vindictive hubs partaking in course disclosure is decreased in course revelation stage, so the reliability of course is improved. These advantages lessen the unfriendly effect of pernicious hubs on network correspondence. Apparently, this trust-based probabilistic transmission plot is the initial chance to be proposed around here. The principle commitments of this paper incorporate 1) A light-weight trust the board model is utilized to assess the reliability of hubs by joining direct and suggested trust proof. The weight coefficient is progressively determined with an original technique to further develop assessment precision particularly on account of experiencing information sparsity issue. 2) RREQ choice system dependent on rebroadcast delay is proposed, in which rebroadcast delay is determined dependent on the dependability of hubs. A hub is permitted to get a few duplicates of RREQ bundles and select one to advance. 3) A trust-based strategy is created for the computation of rebroadcast likelihood. The technique considers the reliability of both the past hand-off hub and the uncovered neighbors. A higher trust level prompts a higher rebroadcast likelihood. TPB plot is unique in relation to conventional trust-based directing plans [13], [14]. TPB keeps malevolent hubs from course disclosure. Notwithstanding, the customary trust-based directing plans don't consider hubs' dependability in the RREQ conveyance stage. The remainder of the paper is coordinated as follows. Segment II presents the connected work. In Section III, the proposed trustbased probabilistic broadcast scheme for mobile ad hoc networks is described in detail. The performance evaluation is discussed in Section IV. Finally, Section V concludes this paper.

OBJECTIVE

The target of the task The RREQ bundle is normally utilized in course disclosure. Indeed, the course is consistently the one engendering way of the RREQ parcel from the source to the objective. Since pernicious hubs debase the organization productivity, they ought to be kept from course disclosure and information transmission

RELATED WORK

The transmission plot is one of the significant systems in portable impromptu organizations [3], [4]. A direct method for executing broadcasting is visually impaired flooding [15], in which each hub rebroadcasts bundles at whatever point it gets a new one. In any case, blind flooding produces repetitive transmissions and may cause the transmission storm issue [7].
Numerous productive transmission plans are proposed as of late. In [16]–[18], just a few chose hand-off hubs are permitted to rebroadcast bundles, with the goal that the quantity of excess transmissions is diminished. To accomplish this, prevailing pruning is proposed to lessen the complete number of hand-off hubs, in which 2-bounce neighbor data is used in the determination of transfer hubs. Nonetheless, its trouble is to acquire the forward-thinking 2-bounce neighbor information in profoundly unique organizations. Reference [19] propose a bi-directional stable correspondence transfer hubs choice plan (BDSC) for multi-bounce broadcasting conventions, where hand-off hubs are chosen dependent on the assessed connect characteristics and the distance between the source telecaster and the possible forwarders. Be that as it may, inability to get communicated parcels by a transfer hub can significantly influence the unwavering quality of the transmission conspire. To defeat such an issue, reference [20] proposed a technique to choose some extra hand-off hub, in order to cover 2-jump transfer hubs m occasions. Thusly, the unwavering quality of parcel conveyance is additionally improved. Associated Dominating Set (CDS) [21] is one more technique to choose transfer hubs. Albums is the virtual spine of specially appointed organizations that can be developed by worldwide or nearby geography data. Nonetheless, the issue of observing a base CDS is NP-finished in these deterministic plans. Probabilistic transmission is one more technique to decrease the quantity of hubs taking an interest in communicating, in which each hub rebroadcasts the got parcels with a given likelihood. Tattle [22] is a straightforward probabilistic transmission plot, in which all hubs rebroadcast the principal approaching bundles with a similar fixed likelihood. The creators extended the GOSSIP and proposed another plan named GOSSIP(p, K) [11] to improve network availability. The improvement is that the hubs in the primary k bounces of the source hub rebroadcast the parcels with a likelihood equivalent to
1. Other than a decent worth, the rebroadcast likelihood can not set in stone adaptively dependent on the nearby or worldwide organization boundaries. In [23], the uncovered neighbor set is thought of. The got likelihood is corresponding to the size of the uncovered neighbor set, to arrive at more extra neighbor hubs by one retransmission. In [24], a neighbor inclusion based probabilistic transmission conspire is proposed for diminishing control overhead in portable specially

appointed TPB for MANETs

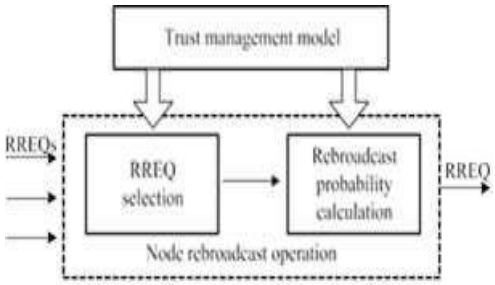

FIGURE 1. Architecture of TPB. networks.

The plan ascertains the rebroadcast likelihood with thought of both the quantity of retransmissions and organization network by joining the extra inclusion proportion and availability factor. To acquire extra neighbor inclusion proportion, creators further modify the transmission request as indicated by rebroadcast delay. Distance data is likewise utilized as a boundary in deciding the rebroadcast likelihood [25]–[29]. In [26], [27], Euclidean distance is taken on to ascertain the rebroadcast likelihood. Rebroadcast likelihood is by and large relative to the Euclidean distance to stay away from excess retransmissions. Nonetheless, the hindrance of Euclidean distance is the requirement for a situating framework. In [28], creators exhibited that the Jaccard distance could be utilized to gauge the Euclidean distance between two hubs without the assistance of the situating framework. In light of the Jaccard distance, probabilistic transmission plans are proposed to work on the disclosure period of responsive specially appointed steering conventions. The two plans decide rebroadcast likelihood as a component of the Jaccard distance. Other than neighbor data [23], [24], [30], hub thickness [30], [31], portability level [32] and remain energy [4] are likewise used to determine rebroadcast likelihood. The current transmission plans work adequately dependent on the joint effort between hubs. No writing has thought about hub dependability when deciding rebroadcast likelihood. In any case, a hub might act perniciously because of the attributes of versatile specially appointed organizations, for example, asset limitations and restricted actual assurance [33]. Malevolent hubs can obliterate the viability of the probabilistic transmission component. To mitigate this issue, the trust level of hubs is considered as a basic boundary in the computation of rebroadcast likelihood for versatile hubs in threatening conditions.

PROPOSED MODEL

TPB conspire contains three fundamental parts: trust the executives model, RREQ choice and rebroadcast likelihood computation. As displayed in Figure 1, the trust the board model is answerable for assessing the dependability of hubs. It gives v_{ij}, t_{ij}, s_{ij}, β_{ij} data to different parts. In the RREQ determination part, a hub is permitted to get a few duplicates of a RREQ prior to performing rebroadcast activity. Each duplicate is appointed a transmission postpone clock dependent on the trust level of the parcel's sending hub. Just the bundle whose clock is first lapsed acquires the capability to be sent. Thusly, the rebroadcast request of RREQs is modified. In the rebroadcast likelihood estimation part, hubs ascertain rebroadcast likelihood as indicated by the trust data of neighbors, and rebroadcast the chose RREQ as per the got rebroadcast likelihood.

LIGHT-WEIGHT TRUST MANAGEMENTMODEL

This paper just considers the bundle sending stage assaults, including parcel dropping assault and adjustment assault. • Packet-dropping assault: a hub might drop bundles going through it to destroy network correspondence. Since hubs may not advance steering parcels in probabilistic broadcast-based course disclosure, just information bundle dropping is considered in this paper. • Modification assault: a hub may illicitly adjust the bundle going through it including information parcel and control parcel. To adapt to the above enemy assault model, we plan a light-weight trust the board model as per existing modes[13], [14], [34]–[37]. The proposed model determines hubs' trust level dependent on two kinds of trust, direct trust from direct perceptions and circuitous trust suggested by the third hub. To gather trust proof, versatile hubs ought to have the option to work in purported unbridled mode, so the sender hub could overhead the retransmission of any parcels by the beneficiary hub [38]. The fundamental parts are outlined in Figure 2. The trust assessment is made occasionally with a predefined time frame. Trust in MANETs is the assessment held by one hub (known as assessing hub) about another hub (known as assessed hub), in light of hubs' authentic practices. To aggregate trust proof acquired in various periods, the Bayesian measurable methodology is sent to assess direct trust, which is accepted to follow a beta likelihood appropriation f (p|α, β). where Γ() is Gamma work, an and β are the super- param-eters to control the dispersion

shape. In the trust oversee ment model, we use αij to address the quantity of positive perceptions (ordinary information bundle sending) the assessing hub I hang on the assessed hub j, and βij addresses the quantity of negative perceptions, including information parcel drop-ping or unlawful alteration. The immediate trust hub I hang on j can be figured from these boundaries as the assumption for beta conveyance. The importance of evidence changes over time. Observations obtained in early time have less influence on the evaluation results. To achieve this, a decay factor, denoted as μ,

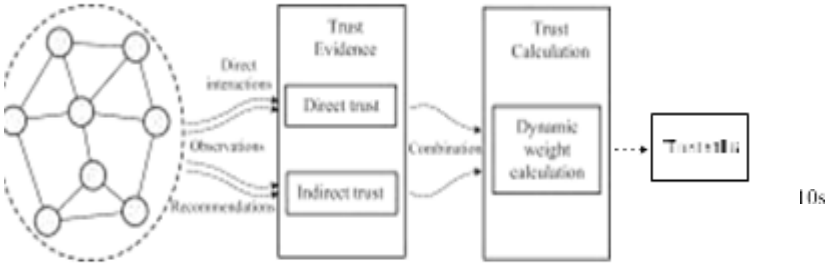

FIGURE 2. Trust management model.

SIMULATION RESULTS

The NS-2 test system with a variant of 2.33 is utilized as the plat-structure to assess the exhibition of steering conventions. The proposed trust-based probabilistic transmission conspire (TPB) is accomplished by adjusting the source code of Ad Hoc On-request Distance Vector steering (AODV) convention [5]. The adjustment is finished with the accompanying four viewpoints. Initially, the light-weight trust level administration model is coordinated into AODV convention, with the goal that hubs can assess the trust level of their adjoining hubs. Also, a trust-based RREQ choice system is utilized to supplant the exemplary first-start things out served sending approach after getting RREQ bundles. Thirdly, hubs forward RREQ dependent on a trust probabilistic transmission model. At long last, the configuration of RREQ and RREPparcels are made of another field to convey course trust data. The exhibition of TPB based convention is contrasted and unadulterated AODV, trust-based AODV (TAODV) [13] and Jaccard-distance-based probabilistic broadcast conspire (JLinear)[28]. In TAODV, on the off chance that more than one way is accessible, the one with the most noteworthy course trust is chosen. The course trust is equivalent to the trust of the hub with the most reduced trust level on the course. To work with correlation, the trust esteem utilized in TAODV is gotten by the trust model proposed in this paper. In JLinear, a node rebroadcasts the received routing packets with a probability that is equal to its Jaccard distance between the sender node.

In the simulations, mobile nodes are randomly placed in the fields of 1000m 1000m. Every mobile node has a 250 meters transmission range and a wireless bandwidth of 2Mbps. All nodes move according to the random way-point mobility model (RWP) [41], in whichthe moving speed is randomly selected from [0m/s, max-speed] and the pause time is set to 10 seconds. The simulation considers constant bit rate (CBR) data traffic between source-destination connec- tions. Each source node sends five CBR packets with a size of 512 bytes per second. The MaxDelay is set to 0.01 seconds, which is equal to the default maximum jitter time of sending broadcast packets in the implementation of AODV in NS-2. Thus, the mechanism of rebroadcast delay doesn't create additional postponement in course disclosure. The boundary wcon in (6) is set to 0.8,taking into account that immediate trust is a higherpriority than circuitous trust for trust assessment. The definite reenactment boundaries are recorded.

In the reenactment, portable hubs are arbitrarily chosen as noxious hubs, which can dispatch a change assault and a parcel dropping assault. In the change assault, mali-cious hubs do assaults by illicitly adjusting variable recorded data in information parcel or directing bundle with a prob-capacity between 0.2- 0.4. In the parcel dropping assault, malicious hubs haphazardly dispose of got information bundles with a likelihood between 0.3-0.6. We expect that malignant hub devotedly forward steering bundles with given transmission prob-capacity. The proportion of alteration and parcel dropping assault are 30% and 70%, separately. The underlying trust worth of each hub is 1, that is, the upsides of boundaries α and β are introduced to 1 and 0, separately.

The accompanying four exhibition measurements are utilized to evaluate network execution:

Bundle conveyance proportion. It is the proportion of the quantity of information bundles got by CBR objections to the quantity of information parcelscreated by CBR sources.

Normal rebroadcast proportion. It is the proportion of the quantity of hubs that rebroadcast the bundles to the quantity of

hubs that get the transmission parcels.

Standardized directing overhead. It is characterized as the proportion of the quantity of control bundles (counting RREQ, RREP, RERR, Hello parcels and the bundles conveying backhanded trust) to the quantity of the information parcels conveyed to the objections. At the point when a control parcel is retransmitted, it is considered one transmission.Normal start to finish delay. It is the normal time expected to effectively convey information bundles from CBR sources to objections. Three sorts of recreations are directed. Everyone is intended to assess the effect of one of the accompanying boundaries on the organization execution:

Number of malevolent hubs. We differ the quantity of malevolent hubs from 0 to 30% of versatile hubs to concentrate on the effect of vindictive hubs on the organization execution. In this sort of reproduction, the quantity of versatile hubs and CBR associations are set to 60 and 10, individually.

Number of portable hubs. We differ the quantity of portable hubs from 40 to 100 to assess the effect of organization thickness. In this sort of recreation, the CBR association is set to 10, and the quantity of vindictive hubs is set to 20% of versatile hubs.

Number of CBR associations. The quantity of CBRconnections is differed from 6 to 18 to assess the effect of organization traffic. The quantity of portable hubs is set to 60 and 20% of them are chosen as malevolent hubs.

The reproduction time is set to 500 seconds. To diminish the unsettling influence of arbitrary mistake, every information point is the normal aftereffect of 40 preliminaries of reenactment. The certainty level is 95%, and the certainty span is displayed as an upward bar in the figures.

TRUST LEVEL DISTRIBUTION OFNODES

Complex assaults, for example, plot and bogus suggestion are not considered by the predetermined foe model. There-front, the trust model can recognize the conduct of hubs with restricted mistakes that can be disregarded in TPB. This paper centers around the levelof hubs' reliability since it is utilized to decide rebroadcast likelihood. To look at hubs' trust level, 100 portable hubs are sent in the reenactment, and 30 percent of them are haphazardly chosen as malignant hubs. The trust esteem is refreshed with a time frame seconds. lower trust esteems. Figure 5 shows the trust levels of a "typical hub" (id: 2) and a "malevolent hub" (id: 30). The trust upsides of both ordinary hubs and noxious hubs vacillate with time. The explanation is that "typical hub" may drop parcels because of the blockage and in this manner its trust level is impacted. Interestingly, "malevolent hub" dispatches assaultsdependent on the likelihood, which brings aboutvarious trust levels for vindictive hubs at various occasions.

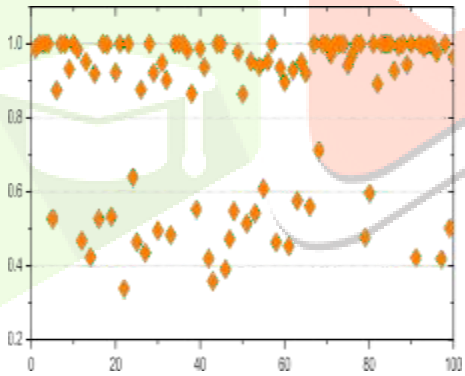

FIGURE 2. Trust values of a normal node and a maliciousnode.

1) VARYING NUMBER OF MALICIOUS NODES Figure 9 shows each of the four conventions experience a ceaseless reduction as far as bundle conveyance proportion as the quantity of noxious hubs increments. The explanation is that malignant hubscould obliterate information transmission by droppingor changing information bundles. In this manner, thepresence of vindictive hubs in versatile impromptuorganizations badly affects the parcel conveyanceproportion. This can be confirmed in Figure 10 appearance the normal course trust level versus the quantity of malevolent hubs. It very well may be seenthat the lower course trust level demonstrates that thecourses have more vindictive hubs overall. In Figure 9, the two TPB and TAODV have a higher parcel conveyance proportion than unadulterated AODV and JLinear under a similar organization conditions. The explanation is that trust the executives model assists the two conventions with building up confided in ways. In these two conventions, TPB accomplishes a clearly higher bundle conveyance proportion thanTAODV. The improvement is primarily because of thecontrast between broadcast plans in the twoconventions. TPB embraces. trust-based probabilistictransmission conspire, in

which a few hubs particularly untrusted hubs broadcast RREQ parcels with a low likelihood. This improves TPB to assemblecourses with a higher trust level than TAODV.Conversely, despite the fact that JLinear is aprobabilistic transmission conspire, it couldn't adapt tonoxious hub. Thusly,the bundle conveyance proportion of JLinear is lower than TPB.

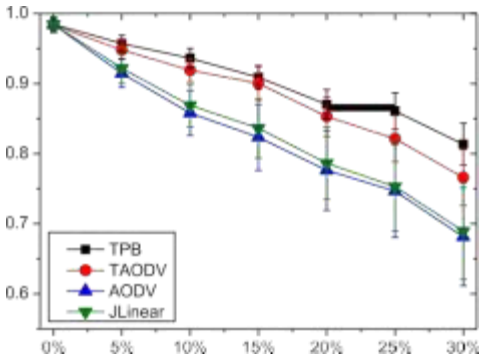

FIGURE 3. Packet delivery ratio with varying number ofmalicious nodes.

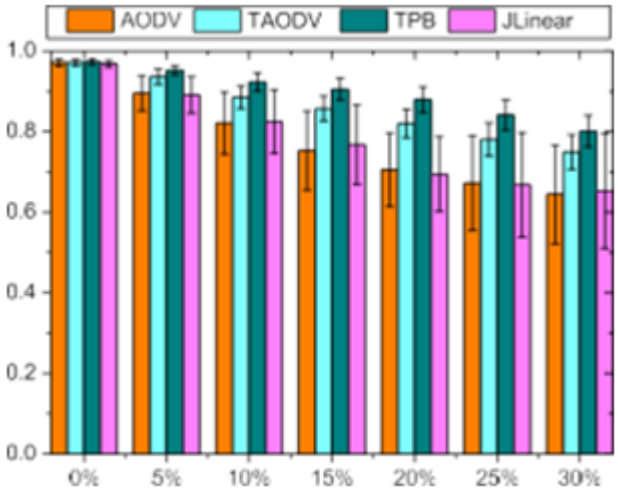

FIGURE 4. Average route trust level with varying numberof maliciousnodes.

The normal rebroadcast proportion with various vindictive hub thickness is displayed in Figure 11. We can see that AODV and TAODV nearly rebroadcast all got steering parcels. Interestingly, TPB and JLinearjust rebroadcast portions of the steering bundles. Since AODV and TAODV accept blind flooding as its transmission strategy, every hub will rebroadcast the directing parcels when initially gets one. Subsequently, the normal rebroadcast proportion of the two conventions is practically equivalent to 100%. TPB spreads steering bundles as per a probabilistic transmission plot, where the rebroadcast likelihood is determined dependent on the trust-value of hubs. In this way, the more the noxious hubs are in the organization, the below normal rebroadcast prob- capacity becomes. Subsequently, the normal rebroadcast proportion diminishes while expanding the quantity of noxious hubs.

SNAPSHOTS

Figure 5: User Register

Figure 6: Adding new server

Figure 7: Sending Keys

CONCLUSION

In this paper, we proposed a Trust-based Probabilistic Broad-cast plot (TPB) to get network correspondence in unfriendly organization conditions. We originally planned a light-weight trust the executives model to assess hub trust-value, in view of chronicled connections between hubs Then we proposed a technique dependent on hubs' dependability to ascertain rebroadcast delay, which is utilized to decide the sending request of directing parcels and hence elevate them to be sent by confided in hubs. We likewise viewed as hubs' dependability when ascertaining rebroadcast likelihood to forestall untrusted hubs from taking an interest in course disclosure. These methodologies give TPB plot the capacity to find entrusted courses with less steering overhead. Recreation results show that TPB based convention can accomplish an altogether higher bundle conveyance proportion and a clearly lower standardized steering overhead, contrasted and blind flooding-based conventions. The upgrades demonstrate that TPB plan can sift through untrusted hubs and lighten the harm from them, in the meantime, decreasing the directing overhead brought about by them.

Future Enhancement

The future work lies in two perspectives. First and foremost, multifaceted trust the executive's model will be additionally contemplated, in order to give precise trust esteem in complex conditions. Also, other than hubs' trust level, different boundaries, similar to hub cave sity, network math can be considered to additionally further develop broadcast effectiveness.

REFERENCES

1. Y. Zou, X. Wang, and L. Hanzo, ''A survey on wireless security: Technical challenges, recent advances and future trends,'' Proc. IEEE, vol. 104, no. 9,pp. 1727–1765, May 2016.
2. A. Galaviz-Mosqueda, M. Morales--Sandoval, S. Villarreal-Reyes,
3. H. Galeana-Zapién, R. Rivera-Rodríguez, and M. Alonso-Arévalo, ''Multi-hop broadcast message dissemination in vehicular ad hoc networks: A security perspective review,'' Int. J. Distrib. Sensor Netw., vol. 13, no. 11, pp. 1–21, Nov. 2017.
4. P. Ruiz and P. Bouvry, ''Survey on broadcast algorithms for mobile ad hoc networks,'' ACM Comput. Surv., vol. 48, no. 1, pp. 1–35, Jul. 2015.
5. D. Reina, S. Toral, P. Johnson, and F. Barrero, ''A survey on probabilistic broadcast schemes for wireless ad hoc networks,'' Ad Hoc Netw., vol. 25, pp. 263–292, Feb. 2015.

6. C. Perkins, E. Belding-Royer, and S. Das, ‘‘Ad hoc on-demand distance vector (AODV) routing,’’ document RFC 3561, 2003, p. 90, vol. 6.
7. D. B. Johnson, D. A. Maltz, and J. Broch, ‘‘DSR: The dynamic source routing protocol for multihop wireless ad hoc networks,’’ Ad Hoc Netw., vol. 5, pp. 139–172, Jan. 2001.
8. S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu, ‘‘The broadcast storm problem in a mobile ad hoc network,’’ Wireless Netw., vol. 8, no. 2, pp. 151– 162, Mar. 2002.
9. Y. Sasson, D. Cavin, and A. Schiper, ‘‘Probabilisticbroadcast for flooding in wireless mobile ad hocnetworks,’’ in Proc. IEEE Wireless Commun. Netw.(WCNC), vol. 2, Jan. 2004, pp. 1124–1130.
10. Y.-H. Chou, T.-H. Chu, S.-Y. Kuo, and C.-Y. Chen,‘‘An adaptive emer- gency broadcast strategy for vehicular ad hoc networks,’’ IEEE Sensors J., vol. 18, no. 12, pp. 4814–4821, Jun. 2018.
11. [10] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze,‘‘The adoption of socio- and bio-inspired algorithms for trust models in wireless sensor networks: A survey,’’ Int. J. Commun. Syst., vol. 31, no. 7, p. e3444,May 2018.
12. Z. Haas, J. Halpern, and L. Li, ‘‘Gossip-based ad hoc routing,’’ IEEE/ACM Trans. Netw., vol. 14, no. 3, pp. 479–491, Jun. 2006.
13. B. Wu, J. Chen, J. Wu, and M. Cardei, ‘‘A surveyof attacks and coun- termeasures in mobile ad hoc networks,’’ in Wireless Network Security. Boston, MA, USA: Springer, 2007.
14. A. M. Shabut, M. S. Kaiser, K. P. Dahal, and W. Chen, ‘‘A multidimen- sional trust evaluation model for MANETs,’’ J. Netw. Comput. Appl., vol. 123, pp. 32–41, Dec. 2018.
15. I. T. Abdel-Halim, H. M. A. Fahmy, and A. M.Bahaa-Eldin, ‘‘Agent-based trusted on-demand routing protocol for mobile ad-hoc networks,’’ Wireless Netw., vol. 21, no. 2, pp. 467–483, Feb. 2015.
16. M. Jacobsson, C. Guo, and I. Niemegeers, ‘‘An experimental investigation of optimized flooding protocols using a wireless sensor network testbed,’’ Comput. Netw., vol. 55, no. 13, pp. 2899–2913, Sep. 2011.
17. M. E. Hoque, F. Rahman, S. K. Kundu, and A. Rahman, ‘‘Enhanced partial dominant pruning (EPDP) based broadcasting in ad hoc wireless networks,’’ in Proc. Int. Symp. Perform. Eval. Comput. Telecommun. Syst.,2009, pp. 143–150.
18. W. Lou and J. Wu, ‘‘On reducing broadcast redundancy in ad hoc wireless networks,’’ IEEE Trans. Mobile Comput., vol. 1, no. 2, pp. 111–122,Apr. 2002.
19. H. Lim and C. Kim, ‘‘Flooding in wireless ad hoc networks,’’ Comput. Commun., vol. 24, nos. 3–4, pp. 353–363, Feb. 2001.
20. Sandoval, S. Villarreal-Reyes, H. Galeana- Zapién, R. Rivera-Rodríguez, and M. Alonso-Arévalo, ‘‘Multi-hop broadcast message dissemination in vehicular ad hoc networks: A security perspective review,’’ Int. J. Distrib. Sensor Netw., vol. 13, no. 11, pp. 1–21, Nov. 2017.
21. P. Ruiz and P. Bouvry, ‘‘Survey on broadcastalgorithms for mobile ad hocnetworks,’’ ACM Comput.Surv., vol. 48, no. 1, pp. 1–35, Jul. 2015.
22. D. Reina, S. Toral, P. Johnson, and F. Barrero, ‘‘A survey on probabilistic broadcast schemes for wireless ad hoc networks,’’ Ad Hoc Netw., vol. 25, pp. 263–292,Feb. 2015.
23. C. Perkins, E. Belding-Royer, and S. Das, ‘‘Ad hoc on-demand distance vector (AODV) routing,’’ document RFC 3561, 2003, p. 90, vol. 6.
24. D. B. Johnson, D. A. Maltz, and J. Broch, ‘‘DSR: The dynamic source routing protocol for multihop wireless ad hoc networks,’’ Ad Hoc Netw., vol. 5, pp. 139–172, Jan. 2001.
25. S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu, ‘‘The broadcast storm problem in a mobile ad hoc network,’’ Wireless Netw., vol. 8, no. 2,pp. 151–162, Mar. 2002.
26. Y. Sasson, D. Cavin, and A. Schiper, ‘‘Probabilistic broadcast for floodingin wireless mobilead hoc networks,’’ in Proc. IEEE Wireless Commun. Netw. (WCNC), vol. 2, Jan. 2004, pp. 1124–1130.
27. Y.-H. Chou, T.-H. Chu, S.-Y. Kuo, and C.-Y.Chen, ‘‘An adaptive emer- gency broadcast strategy forvehicular ad hoc networks,’’ IEEE Sensors J., vol. 18, no. 12, pp. 4814–4821, Jun. 2018.
28. H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, ‘‘The adoption of socio- and bio-inspired algorithms for trust models in wireless sensor networks: A survey,’’ Int. J. Commun. Syst., vol. 31, no. 7, p. e3444,May 2018.
29. Z. Haas, J. Halpern, and L. Li, ‘‘Gossip-based ad hoc routing,’’ IEEE/ACM Trans. Netw., vol. 14, no. 3, pp. 479–491, Jun. 2006.
30. B. Wu, J. Chen, J. Wu, and M. Cardei, ‘‘A survey of attacks and counter measures in mobile ad hoc networks,’’ in

Wireless Network Security Boston, MA, USA: Springer, 2007.

31. A. M. Shabut, M. S. Kaiser, K. P. Dahal, and W. Chen, ‘‘A multi-dimensional trust evaluation model for MANETs,’’ J. Netw. Comput. Appl., vol. 123, pp. 32–41, Dec. 2018.
32. I. T. Abdel-Halim, H. M. A. Fahmy, and A. M. Bahaa-Eldin, ‘‘Agent-based trusted on-demand routing protocol for mobile ad-hoc networks,’’ Wireless Netw., vol. 21, no. 2, pp. 467–483, Feb. 2015.
33. M. Jacobsson, C. Guo, and I. Niemegeers, ‘‘An experimental investigation of optimized flooding protocols using a wireless sensor network testbed,’’Comput. Netw., vol. 55, no. 13, pp. 2899–2913, Sep. 2011.
34. M. E. Hoque, F. Rahman, S. K. Kundu, and A. Rahman, ‘‘Enhanced partial dominant pruning (EPDP) based broadcasting in ad hoc wireless networks,’’ in Proc. Int. Symp. Perform. Eval. Comput. Telecommun. Syst.,2009, pp. 143–150.
35. W. Lou and J. Wu, ‘‘On reducing broadcast redundancy in ad hoc wireless networks,’’ IEEE Trans. Mobile Comput., vol. 1, no. 2, pp. 111–122, Apr. 2002.
36. H. Lim and C. Kim, ‘‘Flooding in wireless ad hocnetworks,’’ Comput. Commun., vol. 24, nos.