ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

Re-joining of Authorized Nodes in MANETs using Group Key Management

Tejpreet Singh[1], Dr. Jaswinder Singh[2], Dr. Sandeep Sharma[3]
Research Scholar, Department of CSE, I.K.G-PTU, Kapurthala, India[1]
Associate Professor, Department of ECE, BCET, Gurdaspur, India[2]
Professor, Department of CSE, GNDU, Amritsar, India[3]

Abstract: One of the specially designated versatile networks, commonly referred to as MANET, performs on the basics that each and every one grouping in nodes totally operate in self-sorting out limits. In any case, performing in a group capacity maximizes quality and different sources. Mobile ad hoc network is a wireless infrastructureless network. Due to its unique features, various challenges are faced under MANET when the role of routing and its security comes into play. . The review has demonstrated that the **impact of failures during the information transmission has not been considered in the existing research. The majority of strategies for ad hoc networks just determines the path and transmits the data which prompts to packet drop in case of failures, thus resulting in low dependability.** The majority of the existing research has neglected the use of the rejoining processing of the root nodes network. Most of the existing techniques are based on detecting the failures but the use of path re-routing has also been neglected in the existing methods. Here, we have proposed a method of path re-routing for managing the authorized nodes and managing the keys for group in ad hoc environment. Securing Schemes, named as 2ACK and the EGSR schemes have been proposed, which may be truly interacted to most of the routing protocol. The path re-routing has the ability to reduce the ratio of dropped packets. The comparative analysis has clearly shown that the proposed technique outperforms the available techniques in terms of various quality metrics.

Keywords: MANETs, Re-Routing, Group Key Management, Hybrid based PSO, Reliable Path

I. INTRODUCTION

Mobile based Ad-Hoc system is a continuous self-making and self-checking system which comprises of mobile devices that are associated with the remote medium mode. Every last device has the capacity to move randomly to the entire system, this free mobility thus causes continuous variations of the link among the nodes. At whatever point a device in the system gets a bit of data, it feels uncomfortable to make sense of which the data is connected to it, it can either be utilized to some of the specific devices [7]. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network. A MANET may operate either in isolation, or may be connected to the greater Internet via gateway routers. MANETs have several notable attributes:

- **Multi-hop routing:** If a node wants to send data to another node then it sends data to its adjacent node which in turn forwards the data in the direction of the intended node. Thus, the data is transmitted through several nodes sometimes before it reaches to its destination.
- **Dynamically changing links**: The network has ever-changing topology as the nodes are not fixed and have the freedom to move about anywhere.
- **Distributed/Shared operation:** Since nodes themselves are everything that controls the network and there is no central administrative system thus the control of the network is shared among the nodes.
- **Self-behaving nodes**: All nodes can operate as both router and host

II. GROUP KEY MANAGEMENT

The key administration is a testing in ad hoc networks, as it isn't generally conceivable to guarantee the supply of a resource to every one of the nodes everytime. Accordingly, ad hoc networks can't base its confirmation mechanism in an incorporated and stuck foundation. In addition, ad hoc networks are generally formed by means of nodes with bound devices. Thus, security must be given without enormous power consumption as few nodes can't execute typical complex cryptographic operations.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

On this in the meantime, the group is established with the approved nodes and by distributing the group key time to time. If any one of the approved node does not update himself with the new group key, then the leader of that group will check its old key, sequence number, digital signature and authentication to make it again as approved node. On this, to control group keys inside the ad hoc environment which make utilization of the agreeable Optimized link state Routing Protocol (SOLSR) [2]. The protocol, known as effective establishment key administration for comfortable Routing (EGSR), utilizes a little scope of messages for the association key conveyance technique to diminish the quality utilization. EGSR protocol is made out of 3 basic mechanisms: to begin with, group key circulation; second, a combination of group segments and new nodes joining; third, round leader replacement. In this protocol, the group key is occasionally supplanted to reject non-lawful offense nodes and to stay away from utilization of the same group key in more than some amount of data, when powerless encryptions systems are being used. Our idea is authorizedly coordinated with impromptu patterns, for example, nonattendance of foundation and the consistent group dividers. EGSR does not require a preparatory segment, in which the executive readies a couple of nodes with privileged insights and systems which could upset the complete system if revealed. In our protocol, the greater part of the nodes need public and a private key, a declaration given through to get right of the section to control element (access control entity) and to be on the authorized node rundown to begin the use of the network. The proposed protocol streamlines the prohibition of non-approved nodes and the identification of dreadful behavior. The authorized nodes can re-join the the group, if any authorized not is not ready to get the changed group key.

III. IMAGE OF EGSR MECHANISM

The group key initiates via the round leader and distribution is achieved through a declaration message, which indicates the provision of a new group key. Fig.1 illustrates the mechanism for distribution of group key.

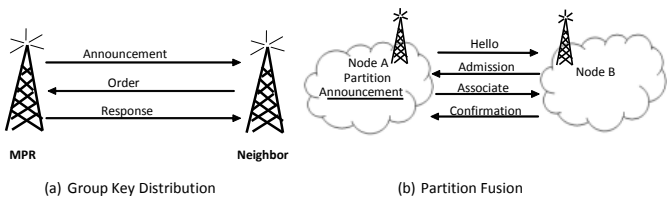

Fig. 1. Mechanism of EGSR

When the round leader neighbors concentrate the announcement, they place the Order message to receive the new group key. The round leader ends the method with sending the reaction message to every neighbor, which contains the new group key encrypted with its neighbors public key.

IV. The 2ACK SHCEME

The essential thought of this scheme is to send two-hop affirmation parcels in the opposite direction of the steering path. With a specific end goal to diminish extra steerage overhead, just a small amount of the received data packets are recognized in the 2ACK plan. In this way, it identifies the misbehaving nodes, take away them and pick the other way to transmit the records. The watchdog discovery mechanism has a low overhead. Unfortunately, the watchdog strategy experiences a few inconveniences such as ambigious collisions, receiver collisions and limited transmission power [3]. The essential issue is that the successful packet reception can be accurately decided at the recipient of the next hop-link, but the watchdog technique only monitors the transmission from the sender of the next hop-link. In the next hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet and it will not be forwarded further. The result is that this connection will be labeled. 2ACK plan fundamentally streamlines the revelation system. Taking note of that a making trouble hub can either be the sender or the collector of the following bounce connect, one should concentrate on the issue of recognizing misbehaving links instead of misbehaving nodes.

V. RELATED WORK

This paper [4] considers the hassle of key agreement in dynamic peer agencies. (Key settlement, specifically in a group setting, is the stepping stone for all other protection services.) Dynamic peer corporations require now not first-rate preliminary key agreement (PKA) however additionally auxiliary key agreement (AKA) operations, which incorporates member addition, member deletion, and institution fusion. We discuss all organization key settlement operations and gift a concrete protocol suite, CLIQUES, which gives entire key agreement services. This paper [5] employs periodic trade of messages to keep topology information of the network at every node. OLSR is an optimization over a pure hyperlink kingdom protocol because it compacts the dimensions of facts dispatched within the messages, and furthermore, reduces the number of re-transmissions to flood those messages in a whole

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

network. This paper [6] proposed an power-inexperienced and scalable group key agreement (GKA) scheme for wi-fi ad-hoc networks, which makes use of a generalized round hierarchical organization version, in which the network is partitioned into subgroups at unique layers and each subgroup is organized in a circle. Next, we describe the computational and communication energy evaluation of a regular node determined in ad-hoc networks and provides some formulation that can be used to calculate the strength intake fees for protocols done the usage of precise microprocessors and radio transceiver modules.This paper [7] describes inexperienced protocols for be part of recent nodes and revocation of compromised nodes. We look at the tool with the useful resource of calculating opportunity of achievement of every operation. We evaluate safety of the system in opposition to outdoor eavesdroppers and talk its safety in opposition to an adversary that corrupts the nodes of the network. This paper [8] displays how our scheme may be blended with the Multipoint Relaying method, in a very effective way, in keeping with the localization of the organization contributors and their mobility. The performance of this mixture in phrases of average latency of key delivery, power intake and key delivery ratio, is proven through simulation. To save network's resources, in [9], a group key agreement method using ECDH (Elliptic Curve Diffie-Hellman) based on GDH.3 (group Diffie-Hellman) protocol is presented, replacing original Diffie-Hellman in GDH.3. Using ECDH in GDH.3 does not change the security performance that's inherence for GDH.3, but it could save network resource consumption during key agreement. This paper[10] proposed a protocol that additionally avoids using a TTP or a central authority and achieves a great power balance. Finally, we evaluate the verbal exchange/computation complexity of our protocol with formerly recognized protocols and display that it compares favorably with them. This paper [11] recommend at ease and green tree-based totally group key control scheme, that is very appropriate for Pay-television structures. In addition to owning the advantages of the previous tree-based scheme, which include O(log N) verbal exchange charge for each group key replace and O(log N) mystery keys for each member, our scheme has tremendous capabilities, in which N is the overall quantity of members. This paper [12] proposed a scheme that saves time and electricity for common cluster updations and key updations. To thrust back the non-organization memberships from interpreting the facts, complicated key referred to as institution key's being generated. The secrecy of the company key's being maintained organization key that avoids the trouble of certificates and 1/3 involvement. This paper [13] explores using batching of institution club adjustments to lessen the time and key re-distribution operations. The talents of ECC protocol are that, no keys are exchanged among existing members at be part of, and simplest one key, the organization key, is introduced to closing people at depart in the protection analysis, our proposed set of guidelines takes a great deal much less time even as customers be a part of or leave the agency in evaluation to present one.

VI. DRAWBACKS OF EXISTING WORK

- The effect of failures during the data transmission has not been considered in the existing research. The majority of techniques for ad-hoc networks just determines the path and transmits the data which leads to packet drop in case of failures, thus resulting in low reliability.

- Most of the existing techniques are based on detecting the failures but the use of path re-routing has also been neglected in the existing methods. The path re-routing has the ability to reduce the ratio of dropped packets.

These problems loose the group management efficiency. The next section has proposed the technique that sorts out the problem of failure of nodes during packet transmission. Fault tolerance is achieved by the use of path re-routing. Re-routing will be done over the node whose successive node has failed. The enforcement of this proposed technique leads to better values of end to end delay and power consumption. The proposed technique is designed and implemented using MATLAB 2013a and the tool used is data analysis toolbox. The proposed technique is also compared with the existing technique to prove that the new technique has a better performance.

VII. PROPOSED TECHNIQUE

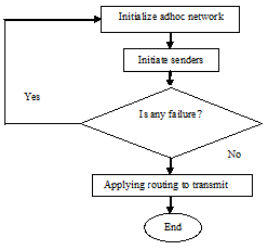

Fig.2. Flowchart of the proposed re-joined authorized nodes technique

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

Step1: Initialize or start the ad hoc network with respect to their characteristics like maximum dimensions, the number of nodes etc.

Step2: Group of authorized nodes will be formed using ASO-PSO technique.

Step3: Group Key will be generated by Round Leader and given to authorized nodes time to time.

Step4: If any authorized node failure is found in that case apply the re-routing process.

The proposed EGSR method says that while we are creating the group with the authorized nodes, the group leader updates the group key time to time, and in case, one of the authorized node is not able to update himself with the new group ke,y then the leader of that group will check its old key, sequence number, digital signature and certificate through ACE to make it again as authorized node.

The EGSR disseminates the group key to all nodes in light of three principle components: the group key dispersion; the new nodes joining; and the leader failure identification and leader substitution.

In EGSR, the group key distribution is initialized in each round by a round leader, and if the round leader fails, it is important to consequently substitute the round leader to proceed the group key distribution.

VIII. ADVANTAGES OF THE PROPOSED TECHNIQUE

- Our said approach decreases the end to end delay and reduces the number of internal attacks.
- Our technique manages the group key distribution and round leader in an efficient way.

IX. SIMULATION RESULTS OF EGSR RE-ROUTING MECHANISM

The simulation results of my proposed technique i.e. Re-joined Authorized Nodes in figure 5, and the existing 1 and existing 2 techniques are shown in figures 3 and 4, where existing1 represents the EGSR operation and existing 2 represents the Authorized Nodes Failure model. In my proposed technique, the authorized nodes are re-joined after the verification of their old key, sequence number and the certificates through ACE by the round leader. The egsr operation simply joins the authorized nodes and provides the path for transmission but does not provide the re-routing mechanism. The delay is high and incurs extra overhead in case of existing techniques. From the simulation model results, it has been found that the re-joined authorized nodes technique has fewer values of delay and overhead as compared to the existing ones.

(A) Efficient Group Key Secured Routing (EGSR) Operation: Existing 1 Technique

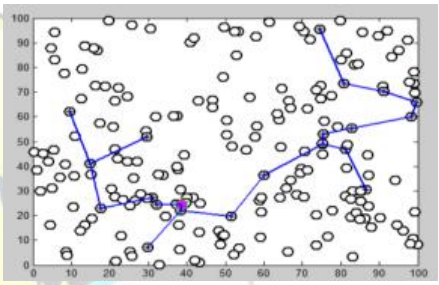

Fig.3. EGSR Operation

(B) Authorized Nodes Failure: Existing 2 Technique

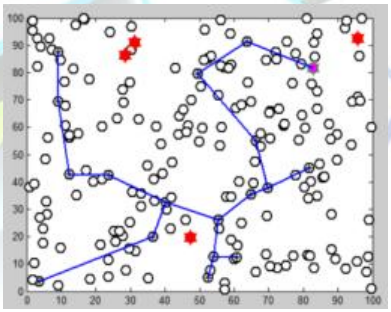

Fig.4. Authorized Nodes Failure

(C) Re-Joined Authorized Nodes: Proposed Technique

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

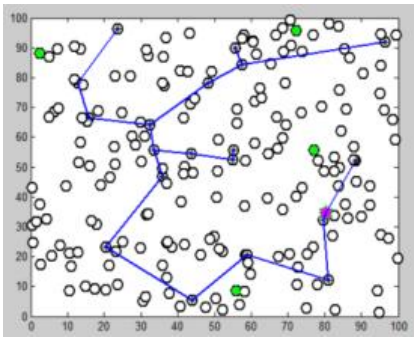

Fig.5. Re-Joined Authorized Nodes

X. COMPARISON OF EXPERIMENTAL RESULTS AND GRAPHICAL ANALYSIS

In this area of the phase, I have symbolized the relative consequences of the simulations demonstrating the viability of the proposed strategy over the existing techniques. The results are taken using MATLAB2013a with the commands revealed in the table below.

TABLE I

SUMMARY OF COMMANDS

Character	Explanation
+	Addition
-	Subtraction
*	Multiplication
/	Division
^	Exponential
:	Creates vectors with equal spaced element
;	End row in array
%	Denotes a comment, specifies output format
()	Encloses elements of array
[]	Encloses matrix elements

The following metrics of my proposed technique is evaluated with the existing techniques in Matlab2013a. The experimental results are displayed below: **where No. of Nodes: (1*x…….n*x, where x=10), Proposed Technique: Re-joined Authorized Nodes, Existing 1: EGSR Operation, Existing 2: Authorized Nodes Failure**

(A) End-to-End delay

This metric can be defined as the basic time taken by the packet to reach at the receiving end. The information packets effectively conveyed to the receiving end are only counted. The lower value of this metric is unquestionably a pointer of the higher execution of the protocol. This metric is averaged complete surviving packets from senders to the receivers.

Table II

NODES VS. END -TO -END DELAY

No. of nodes	Existing 1	Existing 2	Proposed
1	8.5135	5.7809	5.1821
2	11.9211	11.1531	6.9822
3	15.1796	17.5136	8.0700
4	18.5563	24.3300	11.2465
5	22.9983	32.4152	9.6099
6	27.6907	39.9441	12.0533
7	32.4740	47.0701	10.7719
8	37.6595	55.8346	9.6935
9	44.0950	65.8799	11.1352
10	51.1567	76.4018	12.2001
11	59.1592	88.2335	8.9473

Table II displays the comparative results of no. of Nodes vs. Delay which represents a various number of nodes. According to these nodes, different values of delay are taken in proposed, existing 1 and existing 2 techniques respectively. It demonstrates that the delay of my proposed technique is similarly lower than the existing techniques. The graphical analysis of the simulations is shown below.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

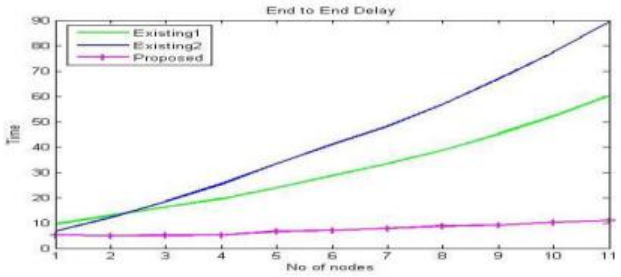

Fig.6. Nodes vs. End To End Delay

(B) Overhead

It is defined as any combination of excess or indirect calculation time, memory, bandwidth alongside different resources that need to achieve a particular objective. Overhead is the overabundance time taken by the protocol to convey the packets to the destination. The routing overhead is characterized as the count of packets utilized for routing in the mobile ad hoc network.

Table III

NODES VS. OVERHEAD

No. of Nodes	Existing 1	Existing 2	Proposed
1	7.5135	4.7810	4.1821
2	10.9211	10.1531	5.9822
3	14.1796	18.5136	7.0700
4	17.5564	23.3300	7.2465
5	20.9983	30.4152	6.6099
6	25.6907	37.9441	9.0533
7	30.4740	45.0701	7.7719
8	35.6595	53.8346	9.6935
9	41.0950	62.8799	8.1352
10	48.1567	73.4018	9.2001
11	56.1593	85.2336	9.9473

Table III displays the comparative results of no. of Nodes Vs Overhead which represents a various number of nodes. According to these nodes, different values of overhead are taken in proposed, existing 1 and existing 2 techniques respectively. It demonstrates that the overhead of my proposed technique is similarly lower than the existing techniques. The graphical analysis of the simulations is shown below.

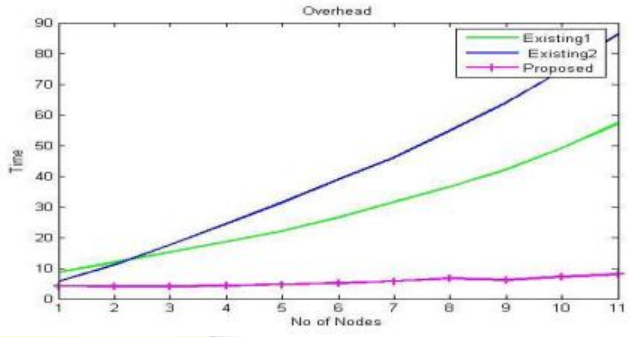

Fig.7. Nodes vs. Overhead

XI. CONCLUSION

The concept of path re-routing has been described in this chapter. The authorized nodes get rejoined after the verification of the old key, sequence number, digital signature and certificate through ACE to make it again as authorized node. Wi-fi specially appointed systems are a guardian breed to versatile ad hoc systems, containing various mobile nodes prepared to do progressively trading records among nodes without requesting a concentrated base. Re-directing based Hybrid ACO-PSO principally based steering set of guidelines for MANETs have been said in this work and is considered for looking at its general execution. This arrangement of standards is material to multi-bounce ad hoc systems with the goal of updating the execution of the overall protocol for portable specially appointed group. The Re-steering based Hybrid methodology is progressed and conveyed the utilization of MATLAB 2013a and the tool compartment utilized is records examination tool compartment. The general execution is assessed by assessing the system that as of now exists to the main is proposed in this work. The impacts have demonstrated that the new methods beat the past methodology.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

REFERENCES

[1] H. Kazemi, et al., "MMAN – A Monitor for Mobile Ad Hoc Networks: Design, Implementation and Experimental Evaluation," The Third ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH 2008), September 2008.

[2] O. C. M.Bandeira Duarte and N. C.Fernandes"An Efficient Group Key Management for Secure Routing in Ad Hoc Networks" GTA/PEE/COPPE - Universidade Federal do Rio de Janeiro Rio de Janeiro, Brazil, 2009.

[3] CharlesE.Perkins,PravinBhagwat,"HighlydynamicDestination Sequenced Distance-Vector Steering (DSDV) for mobile computers", ACM SIGCOMM Computer Communication Review, Vol. 24, no. 4, pp. 234-244, Oct, 1994.

[4] G. Tsudik,M. WaidnerandM. Steiner "Key agreement in dynamic peer groups," IEEE Transactions on Distributed Systems and Parallel System, vol. 11, no. 8, pp. 769–780, Aug. 2000.

[5] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, Oct. 2003.

[6] C. H. Tan and J. C. M. Teo, "Energy-efficient and scalable group key agreement for large ad hoc networks," in 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN'05), 2005, pp. 114–121.

[7] R. Safavi-Naini,L. Luo, W. Susilo and J. Baek,"Self-organised group key management for ad hoc networks," in ACM Symposium on Information, computer and communications security (ASIACCS'06), Mar. 2006, pp. 138–147.

[8] I. Chrisment,O. Festor and M. S. Bouassida, "Efficient group key management protocol in MANETs using the multipoint relaying technique," in Intl. Conference on Networking, Intl. Conference on Mobile Communications, Intl. Conference on Systems and Learning Technologies (ICN/ICONS/MCL 2006), Apr. 2006, pp. 64 – 71.

[9] Q. Niu, "Study and implementation of a improved group key protocol for mobile ad hoc networks," in 8th ACIS International Conference on Artificial Intelligence,Parallel/Distributed Computing,Software Engineering and Networking (SNPD 2007), vol. 1, July 2007, pp. 304–308.

[10] E. Konstantinou, "Cluster-based group key agreement for wireless ad hoc networks," in 3rdInternational Conference on Reliability,Security and Availability(RESA 08), Mar. 2008, pp. 550–557.

[11] Kuei-Yi Chou, Yi-Ruei Chen and Wen-GueyTzeng "An efficient and secure group key management scheme supporting frequent key updates on Pay-TV systems" in Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific.

[12] S. Prasanna,N. Balaji and M. RamyaPriyadharshini, "Energy and mobility based group key management in mobile ad hoc networks" Recent Trends in Information Technology (ICRTIT), 2014 International Conference.

[13] C. Rama Krishna and S. Sharma "An Efficient Distributed Group Key Management Using Hierarchical Approach with Elliptic Curve Cryptography" Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference