TO DETECT AND IDENTIFY NETWORK ATTACKS IN WIRELESS SENSOR NETWORK

1st Ms.M.Juno Isabel Susinthra MCA, M.PHIL, (Ph.D),Assistant Professor ,Department of Computer Science
2nd Ms.P.Nandhitha M.Sc., (Computer Science)
Bon Secours College for Women, Thanjavur.

ABSTRACT

As portable impromptu system applications are conveyed, security develops as a focal necessity. In this paper, we present the wormhole assault, a serious assault in specially appointed systems that is especially testing to safeguard against. The wormhole assault is conceivable regardless of whether the aggressor has not traded off any hosts, and regardless of whether all correspondence gives realness and secrecy. For instance, most existing impromptu system steering conventions, without some instrument to shield against the wormhole assault, would be not able discover courses longer than a couple of bounces, seriously upsetting correspondence. In the wormhole assault, an aggressor records bundles (or bits) at one area in the system, burrows them (conceivably specifically) to another area, and retransmits them there into the system. The hole assault will frame a real risk in remote systems, significantly against varied specially appointed system steering conventions and space primarily based remote security frameworks. We present a general instrument, called bundle chains, for identifying and, in this way shielding against wormhole assaults, and we present a particular convention, called TIK, that actualizes rope. We likewise talk about topology-based wormhole location, and demonstrate that it is unthinkable for these ways to deal with recognize some wormhole topologies.

I. INTRODUCTION

Most past specially appointed systems administration inquire about has concentrated on issues, for example, directing and correspondence, accepting a confided in condition. Nonetheless, numerous applications keep running in untrusted conditions and require secure correspondence and directing. Applications that may require secure correspondences incorporate crisis reaction activities, military or police systems, depend upon specially appointed systems for correspondence. Applications are developing and far reaching selection is not too far off. We present the general instrument of parcel rope to recognize wormhole assaults, and we present two sorts of rope: geographic chains and worldly rope. We plan a proficient confirmation convention, called TIK, for use with worldly chains. In this paper, we characterize an especially difficult assault to guard against, which we call a wormhole assault, and we present another, general component for recognizing and, accordingly protecting against wormhole assaults. In this assault, an aggressor records a bundle, or individual bits from a parcel, at one area in the system, burrows the parcel (potentially specifically) to another area, and replays it there. Area IV presents chains and talks about a general methodology for distinguishing wormholes. Segment V talks about worldly rope in detail and displays the TIK convention for moment remote communicate validation, and Section VI gives a new valuation of TIK and parcel chains, just as different strategies forwormhole identification. Segment VII examines related work, and Section VIII introduces our decisions. The guarantee of portable impromptu systems to take care of difficult true issues keeps on pulling in consideration from mechanical and scholarly research ventures. We likewise break down other discovery approaches, for example, topology-based wormhole location, and demonstrate that topology-based recognition can't identify a few wormholes. We center our exchange in this paper on remote specially appointed systems,

however our outcomes are pertinent all the more extensively to different sorts of systems, for example, remote neighborhood (LANs) and cell systems. Area II of this paper introduces the wormhole assault and talks about how the wormhole assault can be utilized against specially appointed system directing conventions. In Section III, we present our suppositions.

II. PROBLEM STATEMENT

It is additionally workable for the assailant to forward each bit over the wormhole specifically, without trusting that a whole bundle will be gotten before starting to burrow the bits of the parcel, so as to limit delay presented by the wormhole. Because of the idea of remote transmission, the aggressor can make a wormhole notwithstanding for parcels not routed to itself, since it can overhear them in remote transmission and passage them to the conniving assailant at the contrary end of the wormhole. In the event that the aggressor plays out this burrowing sincerely and dependably, no damage is done; the assailant really gives a valuable administration in associating the system all the more effectively. Be that as it may, the wormhole puts the aggressor in an amazing position in respect to different hubs in the system, and the assailant could abuse this situation in an assortment of ways.

In a wormhole assault, an aggressor gets bundles at one point in the system, "burrows" them to another point in the system, and after that replays them into the system starting there. For burrowed separates longer than the ordinary remote transmission scope of a solitary jump, it is straightforward for the assailant to influence the burrowed parcel to touch base with preferred measurement over a typical multihop course, for instance, through utilization of a solitary long-extend directional remote connection or through a direct wired connect to an intriguing aggressor.

Moreover, the assailant is undetectable at higher layers; in contrast to a vindictive hub in a directing convention, which can regularly effectively be named, the nearness of the wormhole and the two conniving aggressors at either endpoint of the wormhole are not unmistakable in the course. The assault can likewise still be performed regardless of whether the system correspondence gives secrecy and genuineness, and regardless of whether the assailant has no cryptographic keys. Moreover, the assailant is undetectable at higher layers; in contrast to a pernicious hub in a steering convention, which can regularly effectively be named, the nearness of the wormhole and the two conniving aggressors at either endpoint of the wormhole are not unmistakable in the course. For instance, OLSR and TBRPF use HELLO bundles for neighbor location, so if an assailant burrows through a wormhole to a plotting aggressor close hub all HELLO parcels transmitted by hub, and similarly burrows back to the main aggressor all HELLO bundles transmitted by, at that point and will trust that they are neighbors, which would make the directing convention neglect to discover courses when they are not really neighbors. For DSDV, if each directing commercial sent by hub or hub were burrowed through a wormhole between conniving nattackers close to these hubs, as depicted above, at that point and would trust that they were neighbors.

The wormhole assault is especially perilous against numerous specially appointed system steering conventions in which the hubs that hear mama parcel transmission straightforwardly from some hub view themselves as in scope of (and, therefore a neighbor of) that hub. One precedent is any remote access control framework that depends on physical nearness, for example, remote vehicle keys, or closeness and token-based access control frameworks for PCs. Insuch frameworks, an aggressor could hand-off the validation trades to increase unapproved get to. At the point when the goal hub's neighbors hear this REQUEST parcel, they will pursue ordinary steering convention handling to rebroadcast that duplicate of the REQUEST, and afterward dispose of without preparing all other got ROUTE REQUEST bundles starting from this equivalent course For instance, when utilized against an on-request directing convention, for example, dynamic source steering (DSR) or specially appointed on-request separate vector (AODV) an incredible utilization of the wormhole assault can be mounted by burrowing each ROUTE REQUEST bundle specifically to the goal target hub of the REQUEST. Disclosure.

This assault, along these lines, keeps any courses other than through the wormhole from being found, and if the assailant is close to the initiator of the course revelation, this assault can even avoid courses multiple bounces long from being found. Conceivable courses for the assailant to then endeavor the wormhole incorporate disposing of instead of sending all information parcels, subsequently making a changeless refusal of-benefit (DoS) assault (no other course to the goal can be found as long as the aggressor keeps up the wormhole for ROUTE REQUEST bundles), or specifically disposing of or adjusting certain information parcels. The neighbor revelation systems of occasional (proactive) directing conventions, for example, dynamic goal sequenced separate vector (DSDV), enhanced connection state steering (OLSR), and topology communicate dependent on turn around way forwarding(TBRPF) depend intensely on the gathering of communicate bundles as a methods for neighbordiscovery, and are likewise very helpless against this assault. On the off chance that and, in any case, were not inside remote transmission scope of one another, they would be not able impart.

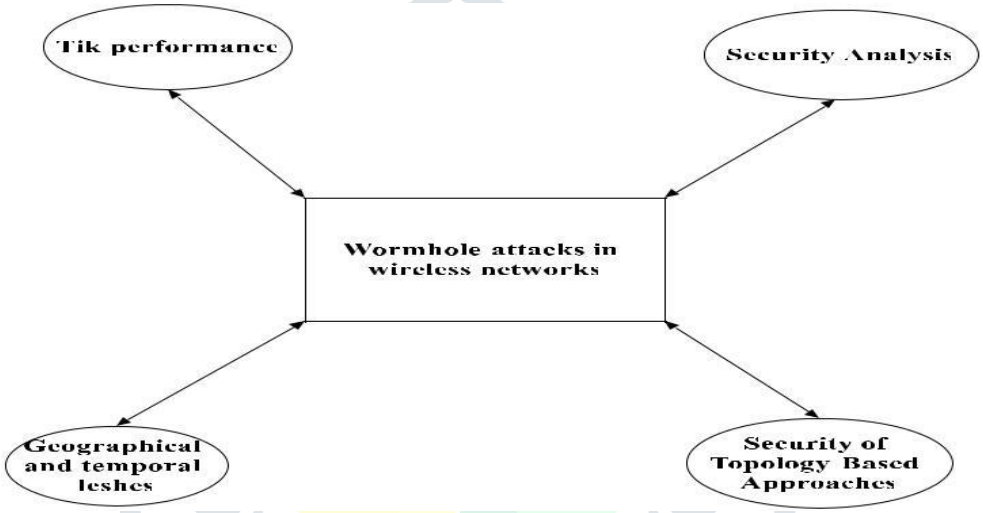

Figure 1. Block Diagram

Besides, on the off chance that the best existing course from towere at any rate bounces long, any hub inside jumps of would be not able speak with, and any hub inside jumps of would be not able speak with. Something else, assume were inside bounces of, yet had a legitimate course to. Since promotes a measurement of 1 course to, would hear a measurement course to. will utilize that course on the off chance that it isn't inside jumps of , in which case there would be a - bounce course from to , and a course of length from to , repudiating the introduce that the best genuine course from to is at any rate jumps long. In every one of these conventions, the wormhole can be utilized to draw in specially appointed system traffic, and can utilize this situation to listen stealthily on traffic, perniciously drop bundles, or to perform man-in the-center assaults against conventions utilized in the system. The wormhole assault is additionally hazardous in different kinds of remote systems and applications.

III. ASSUMPTIONS, NOTATION, AND ATTACKER MODEL

The abbreviation "Macintosh" may all in all mean "medium access control" convention or "message validation code." To evade perplexity, we use "Macintosh" in this paper to allude to the system medium access control convention at the connection layer, and we use "HMAC" to allude to a message confirmation code utilized for verification (HMAC is a specific occasion of a message confirmation code. For reasons, for example, contrasts in remote obstruction, transmit power, or reception apparatus activity, interfaces between hubs in a remote system may now and again effectively work in only one bearing; such a unidirectional remote connection between two hubs and might permit to send bundles to yet not for to send parcels to . As a rule, in any case, remote joins can work as bidirectional connections. A MAC convention by and large is intended to help task over unidirectional connections or is planned just for bidirectional connections; the presentation of our TIK convention does not influence the capacity of the MAC convention to work over unidirectional connections. Security assaults on the remote system's physical layer are past the extent of this paper. Spread-range has been contemplated as a component for anchoring the physical layer against sticking DoS assaults against MAC layer conventions are additionally past the extent of this paper; MAC layer conventions that don't utilize some type of transporter sense, for example, unadulterated ALOHA and Slotted ALOHA, are less powerless against DoS assaults, despite the fact that they will in general utilize the channel less effectively. We expect that the enemy can put hubs at subjective places in the system, and thatthese hubs are associated through a correspondence channel that is inconspicuous by different hubs, however pursues the laws of material science (i.e., messages can't travel quicker than the speed-of-light). We expect that organize hubs are not bargained, but rather we talk about in Section VI-B potential assaults if arrange hubs are imperiled. We accept that the remote system may drop, degenerate, copy, or reorder parcels. We additionally expect that the MAC layer contains some dimension of excess to distinguish haphazardly tainted parcels; in any case, this instrument isn't intended to replace cryptographic confirmation systems.

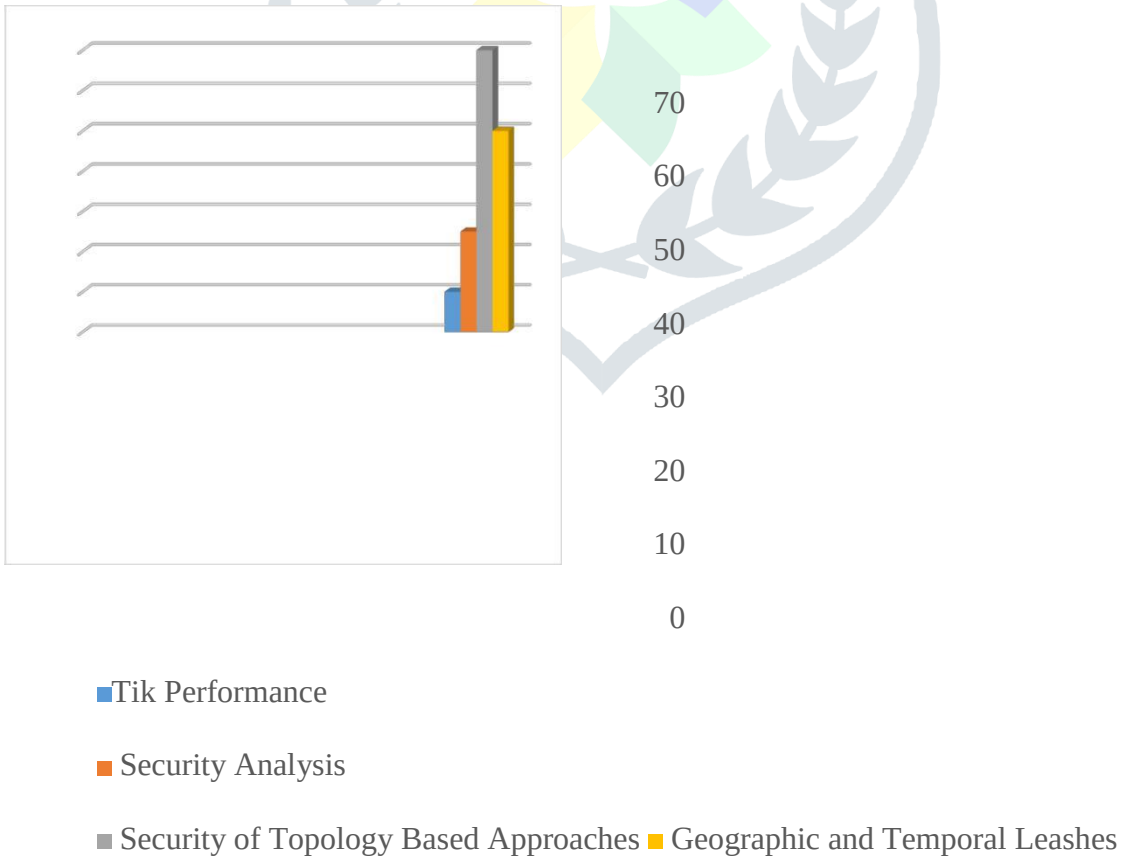

Figure 2. Bar-Chart

We expect that hubs in the system might be asset compelled. Along these lines, in giving for wormhole identification, we utilize effective symmetric cryptography, as opposed to depending on costly hilter kilter cryptographic activities. Particularly on CPU-restricted gadgets, symmetric cryptographic activities, (for example, square figures and hash capacities) are three to four requests of size quicker than hilter kilter cryptographic tasks, (for example, computerized marks). We accept that a hub can acquire a validated key for some other hub. Like open keys in frameworks utilizing lopsided cryptography, these keys in our convention TIK (Section V) are open qualities (when unveiled), in spite of the fact that TIK utilizes just symmetric (not deviated) cryptography. A customary way to deal with this confirmed key dissemination issue is to expand on an open key framework for key circulation; a believed element can sign open key testaments for every hub, and the hubs would then be able to utilize their open key to sign another (symmetric) key being appropriated for use in TIK.

Zhou and Haas propose such apublic-key foundation; Hubaux et al. bootstrap trust connections from PGP-like declarations without depending on a trusted public-key foundation propose asymmetric mechanisms for edge marks for testaments. Alternatively, a believed hub can safely appropriate a verified TIK key utilizing just symmetric-key cryptography ornoncryptographic approaches.

IV. DETECTING WORMHOLE ATTACKS

We recognize land chains and transient rope. A land chain guarantees that the beneficiary of the parcel is inside a specific separation from the sender. A transient rope guarantees that the parcel has an upper bound on its lifetime, which confines the greatest travel separate, since the bundle can go at most at the speed-of-light. Either kind of chain can keep the wormhole assault, since it enables the collector of a bundle to recognize whether the parcel voyaged more remote than the rope permits. in view of the timestamp in the bundle, the nearby get time , the most extreme relative blunder in area data , and the areas of the collector and the sender , then can be limited by .A standard computerized signature plot or other confirmation method can be utilized to empower a recipient to validate the area and timestamp in the got parcel. This methodology is comparative. In specific conditions, bouncing the separation between the sender and collector, , can't avert wormhole assaults; for mexample, In this area, we present the idea of a parcel rope as a general component for distinguishing and, hence protecting against wormhole assaults. A system that utilizes area data to make a land rope could control even these sorts of wormholes. To achieve this, every hub would have a radio engendering model. A collector could check that each conceivable area of the sender (a span around) can achieve each conceivable area of the beneficiary (a sweep around).

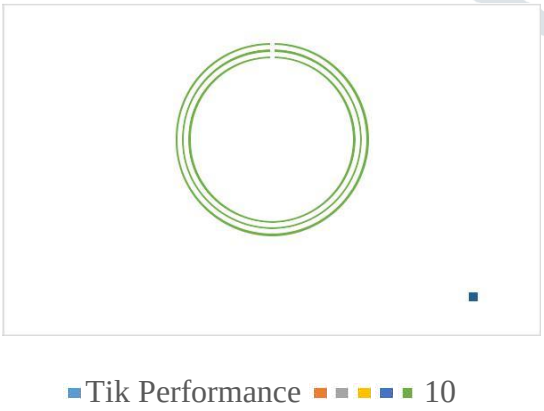

Figure 3. Pie-Chart

A chain is any data that is added to a parcel intended to limit the bundle's most extreme permitted transmission separate. Chains are intended to ensureagainst wormholes over a solitary remote transmission; when parcels are sent over numerous bounces, every transmission requires the utilization of another rope when snags anticipate correspondence

between two hubs that would some way or another be in transmission run, a separation based plan would at present permit wormholes between the sender and beneficiary.

V. TEMPORAL LEASHES

To develop a worldly chain, when all is said in done, all hubs must have firmly synchronized timekeepers, with the end goal that greatest contrast between any two hubs' tickers is. The estimation of the parameter must be known by all hubs in the system, and for fleeting chains, by and large should be on the request of a couple of microseconds or even several nanoseconds. This dimension of time synchronization can be accomplished now with off-the-rack equipment dependent on or on-chip nuclear timekeepers as of now being worked on at NIST in spite of the fact that such hardware isn't at present a typical piece of remote network nodes, it very well may be conveyed in systems today and is required to end up more generally used in future frameworks at decreased expense, size, weight, and power utilization. Despite the fact that our general requirement for time synchronization is to be sure a restriction on the appropriateness of transient rope, for applications that require defense against the wormhole assault, this prerequisite is defended because of the earnestness of the assault and its potential disruption of the planned working of the network. To utilize fleeting rope, when sending a parcel, the sending node incorporates into the bundle the time at which it sent the packet; when getting a parcel, the accepting hub looks at this value to the time at which it got the bundle. The receiver is, consequently, ready to identify if the parcel voyaged excessively far, in view of the asserted transmission time and the speed-of-light. On the other hand, a transient rope can be built by rather incorporating into the bundle a termination time, after which the collector ought not acknowledge the parcel; in view of the permitted most extreme transmission separate and the speed-of-light, the sender sets this lapse time in the parcel as a balance from the time at which it sends the bundle. Similarly as with a land rope, an ordinary advanced mark plot or other validation method can be utilized to enable a collector to verify a timestamp or lapse time in the received bundle.

DISCUSSION

At the point when a genuine hub catches the aggressor professing to be in various areas that would possibly be conceivable if the assailant could go at a speed over the maximum node speed, the authentic hub can utilize
the marked areas to persuade other real hubs that the aggressor is malicious. This utilization of nonrepudiation was additionally proposed by Sirois and Kent. By definition,. Also, when is little, ought to be little, since the calculation a hub uses to decide its area ought to know about physical speed points of confinement of that node. We characterize to be a bound on the most extreme relative position mistake when any hub decides its very own area twice inside a timeframe. Leeway of geological chains over fleeting rope is that the time synchronization can be a lot looser. Another advantage of utilizing topographical chains related to a mark conspire (i.e., a mark giving nonrepudiation), is that an aggressor can be gotten in the event that it claims to dwell at multiple locations. In the event that some hub professes to be at areas.

Furthermore, now and again and, separately, that hub is an aggressor if. A genuine hub distinguishing this from these two bundles can likewise communicate the two parcels to persuade different hubs that the main hub is in fact an aggressor. Every hub hearing these messages can check the two marks, confirm the disparity in the data, and rebroadcast the data on the off chance that it has not recently done as such. To

effectively perform copy concealment in rebroadcasting this data, every hub can keep up a boycott, with each entry in the boycott containing a hub address and the time at which that boycott passage lapses. At the point when a hub gets a message demonstrating an assailant's conduct, it checks if that aggressor is as of now recorded in its boycott. Provided that this is true, it refreshes the lapse time on its present boycott passage and disposes of the new message; else, it includes a new blacklist section and engenders the message.

A potential issue with rope utilizing a timestamp in the parcel is that in a dispute based MAC convention, the sender may not know the exact time at which it will transmit a bundle it is sending. For instance, a sender utilizing the IEEE 802.11MAC convention may not know the time a parcel will be transmitted until the point when around one space time (20 s) preceding transmission. Creating a wasteful computerized signature, for example, RSA with a 1024-piece key, could take three requests of size additional time than this opening time (on the request of 10 ms). The sender, in any case, can utilize two ways to deal with shroud this mark age inertness: either increment the base transmission unit to enable calculation to cover with transmission, or utilize a progressively effective m signature conspire, for example, Schnorr's mark [which empowers productive mark age in the wake of preprocessing. remote flag (i.e., the speed-of-light in air, which is near the speed-of-light in a vacuum). Atthe point when the sender sends the bundle at neighborhood time, it needs to set the parcel lapse time to. At the point when the recipient gets the bundle at nearby time, it further procedures the parcel if the fleeting chain has not lapsed (i.e.,); else, it drops the parcel. This expect the bundle sending and accepting postponement are unimportant, with the end goal that the sender can foresee the exact sending time and the beneficiary can quickly record when the principal bit arrives (or infer amid gathering since the bit rate of transmission is known). The recipient needs an approach to confirm the termination time as generally an aggressor could without much of a stretch change that time and wormhole the parcel the extent that it wants. Two customary methodologies for confirmation come up short for this application. Symmetric message verification codes require private keys to be built up in a system of hubs and have high overhead when utilized for communicate validation, particularly in thick systems, since one authenticator must be incorporated for every goal Digital marks are generally founded on computationally costly hilter kilter cryptography; for instance, the prevalent 1024-piece RSA advanced mark calculation requires about 10 ms on a 800 MHz Pentium III processor for mark age. Since numerous remote applications depend vigorously on communicate correspondence, and since setting up keys is costly, we plan the TIK convention in Section V-C, in view of another convention for proficient communicate verification that all the while gives the usefulness of a transient chain.

VI. RELATED WORK

Wang et al. take note of that the wormhole assault is conceivably increasingly incredible when the assailant has traded off one ormore hubs. Specifically, they recognize open, half-open, and shut wormholes. In this paper, we centeraround open wormholes, where the wormhole does not take part in higher layer conventions, (for example, steering). In a half-open wormhole, one end of the wormhole takes part in a higher layer convention, and may endeavor to cover the presence of the wormhole. At last, in a shut wormhole, the two closures of the wormhole take an interest in the higher layer convention. Our systems enable a higher layer convention to recognize the nearness of open wormholes; extra components inside that higher layer convention are required so as to avoid utilization of half-open and shut wormholes. Hu and Evans propose to utilize directional receiving wires to detect wormhole assaults. Their methodology utilizes an occasional HELLO message to decide the heading to each neighbor. At the point when two hubs and wish to impart, they discover an accurately situated verifier which guarantees that the headings toward and are steady.

What's more, since we know about no distributed explicit subtleties, it is hard to evaluate its security Their methodology is promising; in any case, it depends on impeccably adjusted, totally directional receiving wires, and can't recognize all wormhole occurrences, particularly those utilizing more than one wormhole. Radio recurrence (RF) watermarking is another conceivable way to deal with giving the security portrayed in this paper. RF watermarking validates a remote transmission by regulating the RF waveform in a way known just to approved hubs. RF watermarking depends on keeping mystery the learning of which RF waveform parameters are being regulated; moreover, if that waveform is actually caught at the less than desirable end of the wormhole and precisely duplicated at the transmitting end of the wormhole, the flag dimension of the subsequent watermark is free of the separation it was burrowed.

VII. CONCLUSION

To identify and safeguard against the wormhole assault, we presented parcel rope, which might be either geographic or worldly chains, to confine the most extreme transmission separation of a bundle. At long last, to actualize fleeting chains, we displayed the structure and execution investigation of a novel, effective convention, called TIK, , TIK has computational and memory prerequisites that are effectively satisfiable today; 2.6 MB for hash tree stockpiling speaks to, for instance, under 3% of the standard memory on a Compaq iPAQ 3870 with no outside memory cards, and since the Strong ARM CPU on the iPAQ is fit for performing 222 000 symmetric cryptographic tasks for every second, which likewise gives moment verification of got bundles. TIK requires simply open keys in a system with hubs, and has moderately unobtrusive capacity, per bundle size, and calculation overheads. In this paper, we have presented the wormhole assault, an amazing assault that can have genuine outcomes on many proposed specially appointed system steering conventions; the wormhole assault may likewise be misused in different kinds of systems and applications, for example, remote access control frameworks dependent on physical vicinity. Specifically, a hub needs to perform just somewhere in the range of three and six hash work assessments for each time interim to keep up and coming key data for itself, and approximately 30 hash capacities for each got packet. With item equipment, for example, 11 Mb/s remote connections TIK forces close to a 18% load on CPU time, notwithstanding when overwhelmed with bundles at the greatest speed of the remote system, and regularly utilizes less CPU stack than that in ordinary activity. At the point when utilized related to exact timestamps and tight clock synchronization, TIK canavert wormhole assaults that reason the flag to travel a separation longer than the ostensible scope of the radio, or whatever other range that may be indicated. Adequately tight clock synchronization can be accomplished in a remote LAN utilizing business GPS collectors [39], and remote MAN innovation could be adequately time-synchronized utilizing either GPS or LORAN-C [24] radio signs. A MAC layer convention utilizing TIK productively secures against replay, caricaturing, and wormhole assaults, and guarantees solid freshness. . The overwhelming variable in the ease of use of geographic rope is the capacity to precisely quantify area; since hub development is ease back in respect to the speed-oflight, the impacts of decreased time synchronization exactness are slight. TIK is implementable with current innovations, and does not require critical extra preparing overhead at the MAC layer, since the confirmation of every parcel can be performed on the host CPU. Our geographic chains are less productive than worldly rope, since they require communicate validation, yet they can be utilized in systems where exact time synchronization isn't actually attainable.

VIII. REFERENCE

[1] D. Angluin, J. Aspnes, Z. Diamadi, M. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. Distributed Computing, 18(4):235–253, 2006.

[2] D. Angluin, J. Aspnes, D. Eisenstat, and E. Ruppert. The computational power of population protocols. Distributed Computing, 20(4):279–304, 2007.

[3] B. Awerbuch and S. Even. Efficient associate degreed reliable broadcast is realizable in an eventually connected network. In Proceedings of the 3rd ACM symposium on Principles of distributed computing (PODC), pages 278–281, Vancouver, Canada, 1984. ACM.

[4] H. Baumann, P. Crescenzi, and P. Fraigniaud. Parsimonious flooding in dynamic graphs. In Proceedings of the 28th ACM Symposium on Principles of Distributed Computing (PODC), pages 260–269, Calgary, Canada, 2009. ACM

[5] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint quality model for wireless accidental networks. IEEE Transactions on Mobile Computing, 2(3):257–269, 2003.

[6] M. Biely, P. Robinson, and U. Schmid. Agreement in directed dynamic networks. In Proceedings of the nineteenth International Colloquium on Structural Info and Communication Complexness (SIROCCO), 2012.

[7] B. Bui-Xuan, A. Ferreira, and A. Jarry. Computing shortest, fastest, and foremost journeys in dynamic networks. International Journal of Foundations of applied Science, 14(2):267–285, April 2003.

[8] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine. Maxprop: Routing for vehicle-based disruption-tolerant networks.In Proceedings of the 25th IEEE Conference on Computer Communications (INFOCOM), pages 1–11, Barcelona, Spain, 2006. IEEE.

[9] A. Casteigts, S. Chaumette, and A. Ferreira. Characterizing topological assumptions of distributed algorithms in dynamic networks. In 16th Int. Colloquium on Structural Information and Communication Complexity (SIROCCO), pages 126– 140, Piran, Slovenia, 2009. Springer. (Full version on arXiv:1102.5529). [10] A. Casteigts, P. Flocchini, B. Mans, and N. Santoro. Measuring temporal lags in delay-tolerant networks. IEEE Transactions on Computers, 63(2):397–410, Feb 2014.

[11] A. Casteigts, P. Flocchini, W. Quattrociocchi, and N. Santoro. Time-varying graphs and dynamic networks. International Journal of Parallel, Emergent and Distributed Systems, 27(5):387–408, 2012.

[12] I. Chatzigiannakis, O. Michail, and P. Spirakis. Mediated population protocols. 36th International Colloquium on Automata, Languages and Programming (ICALP), pages 363–374, 2009.

[13] A. Clementi, C. Macci, A. Monti, F. Pasquale, and R. Silvestri. Flooding time in edgemarkovian dynamic graphs. In Proceedings of the 27th ACM Symposium on Principles of distributed computing (PODC), pages 213–222, Toronto, Canada, 2008. ACM.

[14] A. Clementi, A. Monti, F. Pasquale, and R. Silvestri. Information spreading in stationary markovian evolving graphs. In Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on, pages 1–12. IEEE, 2009.

[15] E.W. Dijkstra and C.S. Scholten. Termination detection for diffusing computations. Information Processing Letters, 11(1):1–4, 1980.

[16] C. Dutta, G. Pandurangan, R. Rajaraman, Z. Sun, and E. Viola. On the complexness of knowledge spreading in dynamic networks. In SODA, pages 717– 736, 2013.

[17] A. Ferreira. Building a reference combinatorial model for MANETs. IEEE Network, 18(5):24– 29, 2004.

[18] P. Flocchini, M. Kellett, P. Mason, and N. Santoro. Searching for black holes in subways. Theory of Computing Systems, 50(1):158–184, 2012.

[19] P. Flocchini, B. Mans, and N. Santoro. Exploration of periodically varying graphs. In Proceedings of twentieth International conference on Algorithms and Computation (ISAAC), pages 534– 543, 2009.

[20] P. Flocchini, B. Mans, and N. Santoro. On the exploration of time-varying networks. Theoretical Computer Science, 469:53–68, 2013.