Available Online at http://www.journalajst.com

ISSN: 0976-3376

ASIAN JOURNAL OF
SCIENCE AND TECHNOLOGY

Asian Journal of Science and Technology
Vol. 6, Issue 04, pp. 1349-1353, April, 2015

RESEARCH ARTICLE

PRIVACY WITH LOW OVERHEAD AND SECURE COMMUNICATION FOR HYBRID ADHOC WIRELESS NETWORKS

[1]Aruna, K., [2]Halifath Nisha, A., [3]Jayavani, D., [*, 4]Iswariya, M. and [5]Brindharani, V.

A.V.C College OF Engineering, Mayiladuthurai, Mannampandal– 609 305

ARTICLE INFO

Article History:
Received 11th January, 2015
Received in revised form
15th February, 2015
Accepted 02nd March, 2015
Published online 30th April, 2015

Key words:

Anonymous and secure routing protocols,
Hybrid ad-hoc networks,
Privacy-preserving protocols,
Payment system.

ABSTRACT

In focus of achieving securing communication and protective users' namelessness and site privacy in hybrid spontanepous networks. Symmetric-key-cryptography operations and payment system area unit wont to secure route discovery and information transmission. To cut back the overhead, the payment are often secured while not submitting or process payment proofs (receipts). To preserve users' namelessness with low overhead, we have a tendency to develop economical name generation and trapdoor techniques that don't use the resource-consuming asymmetric-key cryptography. Pseudonyms don't need massive cargo deck or oft contacting a central unit for replenishment. Our trapdoor technique uses solely light-weight hashing operations. this can be vital as a result of trapdoors is also processed by an oversized range of nodes. Developing low-overhead secure and privacy-preserving protocol could be a real challenge due to the inherent contradictions: 1) securing the protocol needs every node to use one each identity, however a permanent identity mustn't be used for privacy preservation; and 2) the low overhead demand contradicts with the massive overhead usually required for protective privacy and securing the communication. Our analysis and simulation results demonstrate that our protocol will preserve privacy and secure the communication with low overhead.

INTRODUCTION

In this paper, we tend to propose a light-weight protocol for securing out institution and information transmission, and preserving users' privacy in hybrid unintentional wireless networks. To preserve users' obscurity, every node uses pseudonyms and one-time session key. Thus, if associate mortal captures a packet, he cannot infer the important identities of the supply, destination, or intermediate nodes. Our protocol permits the nodes to ascertain routes and send/relay packets while not revealing their real identities or the identity of the destination node. A node's pseudonyms will certify it to the intended nodes while not revealing its real identity. Packet tracing is prevented by dynamical the packet's look (bits) at every hop and victimization packet mixers. Therefore, even if an offender eavesdrops on each the supply associated destination nodes, he cannot correlate their packets. To secure the protocol and preserve privacy, the intermediate nodes will ensure that the packets area unit sent by legitimate nodes while not revealing the important identities of the supply and destination nodes. To secure the communication, we tend to use hashing and symmetric-key-cryptography operations and a payment (or incentive) system. The system uses credits (or micropayment) to charge the nodes that send packets and reward those relaying them. The system will stimulate the nodes to relay others' packets to earn credits. Since the nodes get hold of relaying their packets, the system will regulate packet transmission. group action privacy preservation with the payment system is important to achieve acceptance from the users to relay others' packets. Through the payment will make packet relay helpful, most users won't sacrifice their privacy for earning credits.

To reduce the overhead, our protocol avoids the asymmetric-key cryptography as a result of it consumes a lot of resource, will increase the packet delivery delay and degrades the packet delivery quantitative relation (Mahmoud and Shen, 2010). We tend to develop economical nom de guerre generation technique that uses hashing operations. The low overhead of the hashing operations can facilitate reducing the period of time of every nom de guerre and therefore boosting the users' privacy. The end-to-end packet delay will be reduced as a result of pseudonyms area unit quick to calculate and might be pre-computed before receiving the packets. The pseudonyms are echt and invariably synchronic and do not need massive cargo deck or often contacting a central unit for renewal. Trapdoor may be a special token accustomed anonymously inform the destination node regarding the supply node's decision request. It is a key element in any anonymous communication protocol. A trapdoor may be broadcasted throughout the network by an oversized range of nodes. The value of making and processing trapdoors ought to be reduced. We develop efficient trapdoor technique that doesn't need

**Corresponding author: Iswariya, M.*
A.V.C College OF Engineering, Mayiladuthurai, Mannampandal– 609 305

symmetric key operations, however solely light-weight hashing operations. Moreover, a lot of overhead is typically consumed in submitting/ processing payment proofs (or receipts) to secure the payment systems [6]. Our payment system is secured without submitting/processing receipts. Our analysis and simulation results demonstrate that the planned protocol can preserve the users' privacy and secure the communication with low overhead.

Related Works

In [7], incentive mechanism has been projected to stimulate cooperation in multi-hop wireless networks. Rather than mistreatment extensive cryptography to secure the payment, a cheating detection system is employed to scale back the overhead of submitting/processing. Rather than generating a receipt per message or a gaggle of messages, PIS [6], (Mahmoud and Shen, 2010) aims to scale back the receipts' submitting / processing overhead by generating a fixed-size receipt per session. ESIP (Mahmoud and Shen, 2010) proposes a communication protocol that may be used for a payment system with restricted use of asymmetric-key cryptography. The supply and destination nodes generate signatures for only one packet and therefore the economical hashing operations square measure used in the different packets. (Mahmoud and Shen, 2010) propose a payment system for hybrid unexpected networks, wherever each the transmission and downlink packet relay may be multihop. once a route is broken, the nodes that receive the last packet ought to submit receipts to the bottom station to secure the payment.

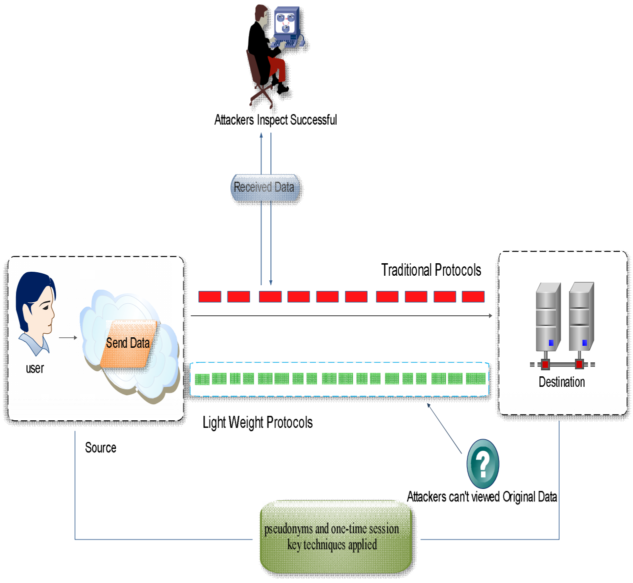
Capkun *et al.* [8] projected a privacy-preserving communication protocol for hybrid accidental network. Each node stores a collection of public/private key pairs and certificates with different pseudonyms signed by a trusty party. The node uses a key try to evidence itself and to share isobilateral keys with its neighbors. It sporadically changes its public/ private key try and shares new isobilateral keys with its neighbors to safeguard its namelessness. The nodes ought to contact the trusty party to refill their certified keys before they are exhausted. every node conjointly stores a routing table which contains the neighbors' pseudonyms and their distances to the bottom station in variety of hops. In ANODR [9], the trapdoor is that the encoding of the destination node's real identity and a random price by using the shared key with the destination node. However, the trapdoor technique is resource overwhelming as a result of every node must try and open the trapdoor with each key it shares with alternative nodes owing to concealment the identities of the source and destination nodes to preserve their namelessness. Moreover, eavesdroppers will trace the packets on the route as a result of their content doesn't amendment at every hop, and they can additionally apprehend if a try of nodes presently communicates.

Proposed Protocol

Pseudonym Generation Technique

The explicit use of a long-run identity or a permanent group of pseudonyms will violate users' privacy. Attackers can link the identity or the pseudonyms to the user, e.g., by analyzing the associated activities. To preserve users' anonymity, every anonym is employed for brief time in such the way that solely the supposed node will link the pseudonyms to every different. By this fashion, although associate degree wrongdoer could link a anonym to the user in one occasion, he cannot violate the user's privacy for a protracted time and cannot like this conclusion within the future owing to pseudonyms' periodic modification and un likability. Using a pseudonym for a protracted time permits attackers to gather much data regarding the visited locations by the anonymous user. Then, by analyzing this data the attackers could determine the users and gain abundant data about their past visited locations. The requirement that a node shouldn't amendment its pseudonym over once before the opposite node changes its anonym, will work well if the 2 nodes exchange packets often. However, in some cases, like route request packets, a node could send multiple packets before receiving a packet from the opposite node. This demand can be relaxed if every node matches the opposite node's pseudonym against a window of L expected anonyms, where L nine two. The node ought to advance the window once it receives a anonym, wherever the last free anonym is

System Architecture


Attackers Inspect Successful
Received Data
Traditional Protocols
user
Send Data
Destination
Light Weight Protocols
Source
Attackers can't viewed Original Data
pseudonyms and one-time session key techniques applied

Security and Privacy Analyses

Communication Security

The per-hop encryption/decryption operations will thwart several attacks. Removing the encryptions and substantiative the correctness of the message implicitly authenticates the intermediate nodes, verifies the hop count, and ensures that the packet is relayed through the route it had been supposed to take. For URREQ and DRREQ packets, the per-hop cryptography operations will secure the routing by preventing manipulating the routing info as well as the identities of the nodes within the route. Moreover, the hop-by-hop encryption/decryption operations build the packets look completely different as they're relayed, which might boost privacy use. In free-riding attack, 2 colluding nodes, e.g., NC1 and NC2, in an exceedingly legitimate session manipulate the packets to piggyback their knowledge to speak freely. The planned payment systems in (Mahmoud and Shen, 2012), [6], [7] use asymmetric-key cryptography to thwart this attack by sign language the messages and substantiative the signatures by intermediate nodes, so that manipulated packets will be detected and born. However, the asymmetric-key cryptography is resource consuming and typically inefficient in protective users' privacy. In our protocol, the per-hop encryption/ decryption operations will thwart this attack as a result of the info sent by NC1 can't be understood by NC2 owing to encrypting (or decrypting) it by a minimum of one intermediate node. The nodes should use the keys shared with the bottom station within the encryption/decryption operations as a result of mistreatment the session keys cannot thwart the attack if there's only 1 intermediate node between colluders: NC1 will piggyback data and encipher the packet with the session key KC1V shared with the victim node Sagebrush State; NV encrypts the packet with the key KVC2Þshared with successive node NC2; the colluding nodes will retrieve the info as a result of they apprehend KC1V and KVC2. The nodes will conspire to earn credits with consuming low resource by relying solely the safety token (e.g., signature) to compose valid receipt rather than relaying the complete packet. Our payment system will guarantee the rationality of packet relaying, encourage the nodes' cooperation, and counteract rational cheating actions while not the overhead of storing, submitting, and processing receipts, as follows:

- The transmission and downlink intermediate nodes area unit motivated to relay the info packets as a result of they're rewarded only the supply base station and destination node receive the packets, and thus packet dropping is AN irrational action.
- 2. Relaying the route discovery packets is useful for the nodes to participate in routes and so earn node to come up with a lot of packets, and so the nodes can earn a lot of credits. Relaying DACK packets is beneficial for the downlink nodes as a result of they're rewarded once the packets reach the bottom station.
- 3. If the supply and destination nodes area unit charged solely for delivered packets, they will communicate freely if the destination node denies receiving the packets or a colluding intermediate node claims route breakage. to stop this, the supply and destination nodes area unit charged for all sent packets. For credit-overspending attack, the nodes could pay more than the quantity of credits they need at the communication time. Most of the present payment systems (Mahmoud and Shen, 2012 and Mahmoud and Shen, 2010) [6], [7] area unit prone to this attack as a result of they use post-paid payment policy, wherever the nodes communicate first and pay our payment system, the bottom stations can thwart this attack as a result of recognize the no dest total credits at the communication time.

For fabrication of route discovery packets, AN wrongdoer tries to fabricate route discovery packets to impersonate a source or a destination node or a base station. This is infeasible in our protocol as a result of the nodes' secret keys should be wont to compose valid packets. For packet-replay attack, attackers could record valid packets and replay them in different locations or time to ascertain sessions beneath the name of others to speak freely or violate user's privacy. In our protocol, the attackers cannot compose URREQ packet with valid timestamp and contemporary anonym without knowing the key keys of the victim nodes. For packet modification attack, if AN wrongdoer manipulates a packet in our protocol, the packet integrity check fails at the base station and destination node. The attackers cannot manipulate the route request packets with success, e.g., by adding or removing nodes' identities, as a result of they are doing not know the nodes' secret keys. In session-hijacking attack, attackers attempt to hijack a session once it's established by legitimate nodes to speak for complimentary. Since the supply node's secret writing is needed in every information packet, the attacker cannot compose valid packets while not knowing the node's secret key and therefore invalid packets may be detected and born. For access management, our protocol ensures that solely legitimate users will access the network to stop unauthorized use. solely legitimate nodes will share keys with base stations and also the nodes cannot communicate while not these keys. For attested packet forwarding, though AN intermediate node shouldn't grasp the identity of the other nodes in a very route, it ought to make sure that it relays packets for legitimate nodes to stop unauthorized use of the network and to make sure that it'll be rewarded for relaying packets. In our protocol, Tp reciprocally authenticates the nodes and base stations, and a base station authenticates every node to its neighbors within the route. With these authentications, every node will make sure that it relays packets sent from legitimate nodes.

Privacy Preservation

For packet correlation, attackers try and correlate the packets sent in one route at totally different hops by finding info that indicate that the packets belong to a similar traffic flow. Attackers can try and correlate packets as follows:

Packet-content correlation: In our protocol, the encryption/decryption operations and ever-changing pseudonyms at every intermediate node guarantee that a packet looks quite totally different because it is relayed from the supply to the destination node. Actually, we have a tendency to create use of the diffusion property of the encoding theme, i.e., encrypting a message M with {different|totally totally different|completely different} keys produces different cipher texts, e.g., though the cipher texts EKAMÞ and EKBMÞ are for a similar message, they appear utterly totally different. Moreover, with victimization secure symmetric-key cryptosystem such as AES, it's computationally unfeasible to correlate the ciphertexts EKAMÞ and EKBMÞ while not knowing the keys Ka and K.

Packet-transmission-time correlation: Attackers might try to correlate a packet because it is relayed by perceptive the transmission time at a node and its neighbors. The attackers build use of the very fact that the nodes typically relay packets when a brief process delay and supported first received-first-relayed basis. ever-changing the packets' look at every hop cannot stop this correlation as a result of it depends on the packets' causing time and not the content. A common approach to change the temporal relationship between the incoming and outgoing packets is to use mixing technique. A mixer buffers a sequence of incoming packets and shuffles them before transmission such correlating the incoming and outgoing packets is troublesome. It can even add dummy packets to the buffer if necessary. The base stations and a few mobile nodes will act as mixers. Privacy is outlined because the protection of knowledge from unauthorized parties. whereas coding will defend the content of the messages, traffic analysis could reveal valuable info regarding the users' relationships, communication activities, and locations.

Location privacy is outlined because the ability to stop attackers from deducing a user's current or past locations whether the precise physical locations or the relative locations in range of hops. Attackers shouldn't be ready to deduce the space to either the anonymous supply or destination node in range of hops, e.g., by analyzing the packets' length or content. In our protocol, the nodes' actual locations aren't used, and therefore the length and content of the route request packets don't reveal the placement of the source nodes as a result of victimisation random-length cushioning and random-value TTL. This may confuse the supply nodes' neighbors whether or not the packets are originated from or relayed by them. The nodes additionally relay the packets destined to them to safeguard their location privacy.

Moreover, the source and destination nodes cannot grasp the locations of each other notwithstanding they're one-hop away. They additionally cannot know whether or not they are within the same cell or not to tell a and identity privacy, a trapdoor that solely the destination node will acknowledge is employed. In our protocol, the trap doorisa contemporary nom de guerre shared between the bottom station and therefore the destination node. Unlinkability of 2 or additional things inside an outlined system implies that this stuff aren't any additional and no less related than they're connected regarding the a priori knowledge. For Source-destination combine unlinkability, although attackers could grasp that a combine of nodes participates in communication activity, they can't make sure that the combine communicates with one another. In our protocol, every time a supply and destination combine communicates, the route discovery packets look completely different, thus linking a packet to a source-destination combine is impossible. Moreover, if an attacker eavesdrops on the supply and destination nodes and their base stations, he cannot ensure that they currently communicate. For supply node and base station unlinkability, if associate degree human eavesdrops on a supply node and its base station, linking the packets is impossible. The packets changed between a supply node and a base station combine at completely different times/sessions are unrelated because pseudonyms are changeable and unlinkable. This means that notwithstanding associate degree human may correlate the combine in one occasion, he cannot enjoy this conclusion in the future. For a transmission and supply node unlinkability, an adversary cannot link a transmission to its supply node because the packets sent in numerous times haven't any common info or any info that may be joined to a true identity. Moreover, characteristic the supply or the destination node doesn't essentially result in characteristic the other party.

Performance Evaluation

To measure the machine times of the cryptanalytic operations needed for our protocol, we've got enforced AES (128 bit key) bilateral key cryptosystem and SHA-1 (160 bit) hash operate victimization the Crypto++5 [23] library and one.6 gigahertz processor. In step with NIST [24], the secure key size ought to be a minimum of 128 bits. The measurement results indicate that a hashing operation needs sixteen.79 Mbytes/s and encryption/decryption operations need 9.66 Mbytes/s. For the energy consumption, the measurements given in [25] indicate that a hashing operation and an encoding or decoding operation need zero.76 J=byte and 1.21 J=byte, severally. These results ensure that hashing and symmetric-key operations need low over head. Table one provides the cryptographical operations needed by our protocol. h, e, and d talk to a hashing, Associate in Nursing coding, and a coding operation, severally. And square measure the numbers of the transmission and downlink nodes together with the source and therefore the destination nodes, severally. The results indicate that our protocol will assign additional overhead to the base stations and it will balance the overhead on the mobile nodes. The bottom stations have additional procedure power and energy than the nodes do. Using NS2, we have a tendency to simulate a hybrid circumstantial network by randomly deploying forty five mobile nodes during a sq. cell of 1200 m. A set base station is found at the center of the cell. The radio transmission vary of the mobile nodes and therefore the base station is one hundred twenty five m. To emulate node quality, we have a tendency to adopt the changed random waypoint model . Specifically, a node travels towards a random destination uniformly elite among the network field; upon reaching the destination, it pauses for a few time; and the process repeats itself later. The node speed is uniformly distributed within the vary [0, 2] m/s and therefore the pause time is three s. The constant bit rate traffic supply is implemente dinevery no deasassociate application layer. The source and destination pairs are every which way elite. Packets are sent at the speed of two packets/s. the quantity of concurrent connections is seven.

The cryptologic operations are simulated by adding their process times to the packets interval. Our simulation is dead for quarter-hour and also the given results are averaged over one hundred simulation runs and conferred with ninety five p.c confidence interval. The length of truncated pseudonyms, Pad, time stamp, real identity, and payload are 10, 2 five, four, 512 bytes, respectively. With these parameters, the network property is 0.96. The property is measured by the quantity of established routes to the quantity of route requests sent by the supply nodes. The simulation results square measure given in Table two. Route establishment delay is that the average measure between sending Associate in Nursing URREQ packet by a supply node and receiving the UREST packet. the information packet delay is that the average time interval between causing an information packet by a supply node and receiving it by the destination node. These delays include: process delays at every node, queuing delay at the interface queue, retransmission delays, and propagation time.

The simulation results indicate that the expected route institution and knowledge transmission delays area unit acceptable because of mistreatment light-weight cryptological operations and pre-computing the pseudonyms. For the RREQ and REST packets, the packet length varies at every node as the packet is relayed, that the average is computed by dividing the number of knowledge relayed in any respect hops by the number of hops. The results conjointly indicate that the overhead of the info packets is thirty six bytes that represent seven p.c of the message size (512 byes). REST packet is massive as a result of it carries the nodes' session keys, however being unicated packet and reducing the packet size at every hop will alleviate this. The packet delivery magnitude relation is that the variety of knowledge packets received by the destination nodes to those sent by the source nodes. Our simulation results indicate that the average packet delivery magnitude relation is zero.95.

Conclusion

Our pseudonym production technique requires only lightweight hashing operations and does not necessitate large storage area or normally refilling pseudonyms from a trusted party. The pseudonyms are authenticated and can be pre-computed to be able to reduce the packet delay. Our evaluations and simulation results demonstrate that the proposed protocol can preserve the nodes' privacy with low overhead and secure the payment, route establishment, and data transmission.

REFERENCES

Mahmoud, M. and X. Shen, 2012. ‘‘FESCIM: Fair, Efficient, Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks,’’ IEEE Trans. Mobile Computer, vol. 11, no. 5, pp. 753-766.

Mahmoud, M. and X. Shen, 2011. ‘‘Lightweight Privacy-Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks,’’ in Proc. IEEE INFOCOM’11-Int’l Workshop Security Computers, Networking Comm. (SCNC), Shanghai, China, pp. 1006-1011.

Mahmoud, M. and X. Shen, 2009. ‘‘Anonymous and Authenticated Routing in Multi-Hop Cellular Networks,’’ in Proc. IEEE Int’l Conf. Comm. (IEEE ICC’09), Dresden, Germany, pp. 839-844.

Mahmoud, M. and X. Shen, 2010. ‘‘PIS: A “Practical Incentive System for Multihop Wireless Networks,’’ IEEE Trans. on Vehicle Technology, vol. 59, no. 8, pp. 4012-4025.

Mahmoud, M. and X. Shen, 2010. ‘‘Stimulating Cooperation in Multi-Hop Wireless Networks Using Cheating Detection System,’’ in Proc. IEEE Conf. Information Comm. (IEEE INFOCOM’10), San Diego, CA, USA, pp. 776-784.

****