SUPERMAN:Security Using Pre-Existing Routing for Mobile Ad hoc Network

Dravya B.C
REVA University

Meenakshi Sundaram.A
School of Computing &
Information Technology
REVA University,Bangalore,INDIA

Abstract : The flexibility and mobility of Ad hoc Networks (MANETs) has been increasing popularly in a wide range of use cases .The networks, security protocols have been developed to protect routing and applications data. However, these protocols only protect routes or communication .Both secure routing and communication security protocols must be implemented to provide full protection .The use of communication security protocols originally developed for Wi-Fi networks can also place a heavy burden on the limited network resources of a MANET .To address these issues, a novel secure framework (SUPERMAN) is proposed. The framework is designed to allow existing network and routing protocols to perform their functions, providing node authentication, access control, and communication security mechanisms, which presents a novel security framework for MANETs, SUPERMAN. Simulation results in comparing SUPERMAN with IPsec, SAODV and SOLSR are provided to demonstrate the proposed frameworks that are suitable for wireless communication security.

Index Terms— access control, authentication, communication system security, mobile ad hoc networks.

1.Introduction

Mobile autonomous networked systems have seen increased usage by the military and commercial sectors for tasks deemed too monotonous or hazardous for humans. An example of an autonomous networked system is the Unmanned Aerial Vehicle (UAV). These can be small-scale, networked platforms. Quadricopter swarms are a noteworthy example of such UAVs. Networked UAVs have particularly demanding communication requirements, as data exchange is vital for the ongoing operation of the network. UAV swarms require regular network control communication, resulting in frequent route changes due to their mobility. This topology generation service is offered by a variety of Mobile Ad hoc Network (MANET) routing protocols [1]. MANETs are dynamic, self-configuring, and infrastructure-less groups of mobile devices. They are usually created for a specific purpose. Each device within a MANET is known as a node and must take the role of a client and a router. Communication across the network is achieved by forwarding packets to a destination node; when a direct source-destination link is unavailable intermediate nodes are used as routers. MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. This can leave MANETs open to a range of attacks, such as the Sybil attack and route manipulation attacks that can compromise the integrity of the network [2].

Eavesdropped communication may equip attackers with the means to compromise the trustworthiness of a network. This is achieved by manipulating routing tables, injecting false route data or modifying routes. Man in the middle (MitM) attacks can be lauched by manipulating routing data to pass traffic through malicious nodes [3]. Secure routing protocols have been proposed to mitigate attacks against MANETs, but these do not extend protection to other data. Autonomous systems require a significant amount of communication [4]. Problem solving algorithms, such as Distributed Task Allocation (DTA), are required to solve task planning problems without human intervention. [4]As a result, these algorithms are vulnerable to packet loss and false messages; partial data will lead to sub-optimal or failed task assignments. This paper proposes a novel security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). The protocol is designed to address node authentication, network access control, and secure communication for MANETs using existing routing protocols. SUPERMAN combines routing and communication security at the network layer. This contrasts with existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network. The organization of chapter is as follows:

Section 1 analyses the problem in the context of previously published work.

Section 2 introduces SUPERMAN, providing a technical discussion of the protocol.

Section 3 outlines the characteristics chosen for modelling, and the results of simulating SUPERMAN compared against selected secure routing and data security protocols.

Section 4 draws conclusions from the research findings.

2.Literature Review

J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.

Unmanned Aerial Vehicles (UAVs) are an emerging technology offering new opportunities for innovative applications and efficient overall process management in the areas of public security, cellular networks and surveying. A key factor for the optimizations yielded by this technology is an advanced mesh network design for fast and reliable information sharing between UAVs. We analyze the performance of our available mesh routing protocol implementations (open80211s, BATMAN, BATMAN Advanced and OLSR) in the context of swarming applications for UAVs. The protocols are analyzed by means of goodput in one static and one mobile scenario using the same embedded hardware platform .

R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in Advanced Computing & Communication Technologies(ACCT), 2012 Second International Conference on. IEEE, 2012, pp. 535–541.

This work introduces NETA, a novel framework for the simulation of communication networks attacks. It is built on top of the INET framework and the OMNET++ simulator, using the generally accepted implementations of many different protocols, as well as models for mobility, battery consumption, channel errors, etc. NETA is intended to become an useful framework for researchers focused on the network security field. Its flexible design is appropriate for the implementation and evaluation of many types of attacks, doing it accurate for the benchmarking of current defense solutions under same testing conditions or for the development of new defense techniques. As a proof of concept, three different attacks have been implemented in NETA. The capabilities of NETA are exhibited by evaluating the performance of the three implemented attacks under different MANET deployments.

S. Maity and S. K. Ghosh, "Enforcement of access control policy for mobile ad hoc networks," in Proceedings of the Fifth International Conference on Security of Information and Networks. ACM, 2012, pp. 47–52.

An ad-hoc network of wireless nodes is a temporarily formed network, created, operated and managed by the nodes themselves. It is also often termed an infrastructure-less, self-organized, or spontaneous network. Nodes assist each other by passing data and control packets from one node to another, often beyond the wireless range of the original sender. The execution and survival of an ad-hoc network is solely dependent upon the cooperative and trusting nature of its nodes .However, this naive dependency on intermediate nodes makes the ad-hoc network vulnerable to passive and active attacks by malicious nodes. A number of protocols have been developed to secure ad-hoc networks using cryptographic schemes, but all rely on the presence of an omni present, and often omniscient, trust authority.
As this paper describes, dependence on a central trust authority is an impractical requirement for ad-hoc networks. We present a model for trust-based communication in ad-hoc networks that also demonstrates that a central trust authority is a superfluous requirement. The model introduces the notion of belief and provides a dynamic measure of reliability and trustworthiness in an ad hoc network.

S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," Ad Hoc Networks, vol. 11, no. 3, pp. 1046–1061, 2013.

Key management (KM) and secure routing (SR) are two most important issues for Mobile Ad-hoc Networks (MANETs), but previous solutions tend to consider them separately. This leads to KM-SR interdependency cycle problem. We propose a KM-SR integrated scheme that addresses KM-SR interdependency cycle problem. By using identity based cryptography (IBC), this scheme provides security features including confidentiality, integrity, authentication, freshness, and non-repudiation. Compared to symmetric cryptography, traditional asymmetric cryptography and previous IBC schemes, this scheme has improvements in many aspects. We provide theoretical proof of the security of the scheme and demonstrate the efficiency of the scheme with practical simulation.

3.Model Overview

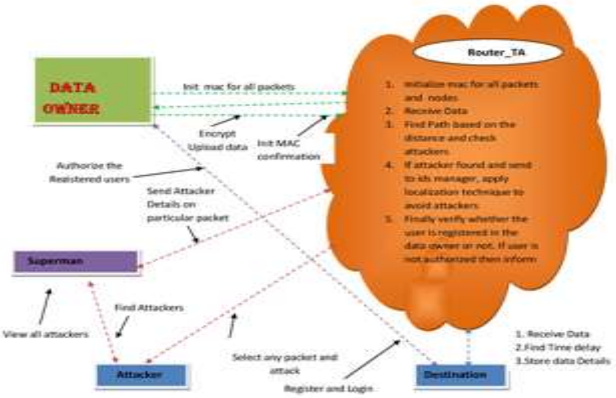
DATA OWNER
Init mac for all packets
Encrypt Upload data
Init MAC confirmation
Authorize the Registered users
Send Attacker Details on particular packet
Router_TA
1. initialize mac for all packets and nodes
2. Receive Data
1. Find Path based on the distance and check attackers
4. If attacker found and send to ids manager, apply localization technique to avoid attackers
5. Finally verify whether the user is registered in the data owner or not. If user is not authorized then inform
Superman
View all attackers
Find Attackers
Attacker
Select any packet and attack
Register and Login
Destination
1. Receive Data
2.Find Time delay
3.Store data Details

Figure1:Architecture Diagram

Every SUPERMAN packet shares a common SUPERMAN packet header (SH), shown in table 1. The data contained in the header can be broken down as follows: x Packet Type denotes the function of the packet x Timestamps provide uniqueness, allowing detection of replayed packets and providing a basis for non-repudiation of previously sent packets x. The protocol identifier indicates the layer 4 type of the encapsulated data. This would be the IP protocol number in an IP based network.

Octets	1	2	3	4
0	Type	Time delay	Time delay	Protocol Identifier

Table 1. SUPERMAN Packet Header (SH) structure.

Key Management SUPERMAN relies on the dynamic generation of keys to provide secure communication. The Diffie-Hellman key-exchange algorithm provides a means of generating symmetric keys dynamically and is used to generate the SK keys. SKb keys can simply be generated by means of random number generation or an equivalent secure key generation service. Secure Node-to-Node Keys SKe keys are used to secure end-to-end communication with other nodes, with one SKe key generated per node, for every other node also authenticated with the network. SKp keys are used for point-to-point security and generated in the same manner as SKe keys. It is important that SKe and SKp keys are different, as the network needs to secure both the content of a packet and the route taken. A KDF can be used to generate these two keys in conjunction with the result of the Diffie-Hellman algorithm, requiring a DKSp/DKSpriv pair, to minimize the cost of security on the network and reduce the key re-use and, in turn the lifetime of each key. These keys are generated when nodes receive DKSp’s from other SUPERMAN nodes. Secure Point-to-Point Footers Secure footers are appended to all communication packets sent between SUPERMAN nodes. SKbp and SKp(x) keys are used in broadcast and unicast integrity service provision respectively. An example tag generation algorithm is the Hashed Message Authentication Code (HMAC) which provides integrity and authenticity services to a packet. A digest of the packet is generated, encrypted with the appropriate key (SKbp or SKp(x)), and appended to the packet. This tag is removed, checked and regenerated at each hop. Secure Broadcast Keys at initialization of the network, the first node to be contacted about joining the network will generate a symmetric network key (SKb). This key is sent to all nodes that authenticate with the network. This key provides the basis for all broadcast communication security in a SUPERMAN network. The SKb is processed by the function KDF(SKb, type) into two broadcast keys (SKbe and SKbp). A node will use these keys to encrypt and sign packets sent to the broadcast address of the network. This key is used for broadcast and multicast communication, such as MANET route updates. It is not used for communication between individual end-points. Upon deriving a broadcast key that will be tied to the network, the receiving node will add the resulting keys to its security table. SKbe keys are used to provide confidentiality to end-to-end broadcast communication. SKbp keys are used to generate tags, generated using an algorithm such as HMAC, appended as a footer to SUPERMAN protected packets, providing broadcast packet integrity. Broadcast keys are generated by the first node to participate in a network joining process as the authenticator (the responding partner). They are then shared as the final stage of all network joining processes that result in a new node becoming a part of that network. Storage SUPERMAN stores keys in each node’s security table. The security table contains the security credentials of nodes with which the node has previously directly communicated, as shown in table 2. This table has n entries, where n is the number of nodes that the node in question has directly communicated with. table 2 shows an example of a security table belonging to node A. It has exchanged credentials with two other nodes, X and Y.

TABLE 2. SUPERMAN Security Table

NodeID	SKe	SKp	DKSp
I(X)	SKe(A,X)	SKp(A,X)	DKSp(X)
I(Y)	SKe(A,Y)	SKp(A,Y)	DKSp(Y)
I(*)	SKbe	SKbp	SKb

The shared symmetric broadcast key (SKb) has two derived forms, the SKbe and SKbp. These are stored in the local security table as a separate broadcast address, denoted by I(*). These keys are not associated with any one network, but represent security credentials held by the whole network. A node's ID would be its address.

4.Our Methodologies

1.Secure Node-to-Node Keys

SKe keys are used to secure end-to-end communication with other nodes, with one *SKe* key generated per node, for every other node also authenticated with the network. *SKp* keys are used for point-to-point security and generated in the same manner as *SKe* keys. It is important that *SKe* and *SKp* keys are different, as the network needs to secure both the content of a packet and the route taken. A KDF can be used to generate these two keys in conjunction with the result of the Diffie-Hellman algorithm, requiring a *DKSp/DKSpriv* pair, to minimize the cost of security on the network and reduce the key re-use and, in turn the lifetime of each key.

2.Secure Broadcast Keys

At initialization of the network, the first node to be contacted about joining the network will generate a symmetric network key (*SKb*). This key is sent to all nodes that authenticate with the network. This key provides the basis for all broadcast communication security in a SUPERMAN network. The *SKb* is processed by the function *KDF(SKb, type)* into two broadcast keys (*SKbe* and *SKbp*). A node will use these keys to encrypt and sign packets sent to the broadcast address of the network. This key is used for broadcast and multicast communication, such as MANET route updates. It is not used for communication between individual end-points.

3.End-to-end Communication

End-to-end security provides security services between source and destination nodes by using their shared SKe Confidentiality and integrity are provided using an appropriate cryptographic algorithm, which is used to generate an encrypted payload (EP). Authenticated Encryption with Associated Data (AEAD) is an example of such an algorithm. AEAD and related cryptographic algorithms provide confidentiality, authenticity and integrity services. The end-to-end element of a SUPERMAN packet is not modified at any point along a route. Its purpose is to provide confidentiality and source authentication services.

4.Point-to-point Communication

When protected, data is propagated over multiple hops, it is authenticated at each hop. This is achieved using a hashing algorithm, such as HMAC. This is applied to the entire packet to provide point-to-point integrity. A tag is generated using the shared SKp of the transmitting node and next hop, which is unique to the direct link in question. The tag is replaced at each intermediate hop, until the destination node is reached. Thus, the authenticity of a route is maintained, as each node on the route must prove their authenticity to the next hop. This tag can also be used for integrity checking.

5.Result

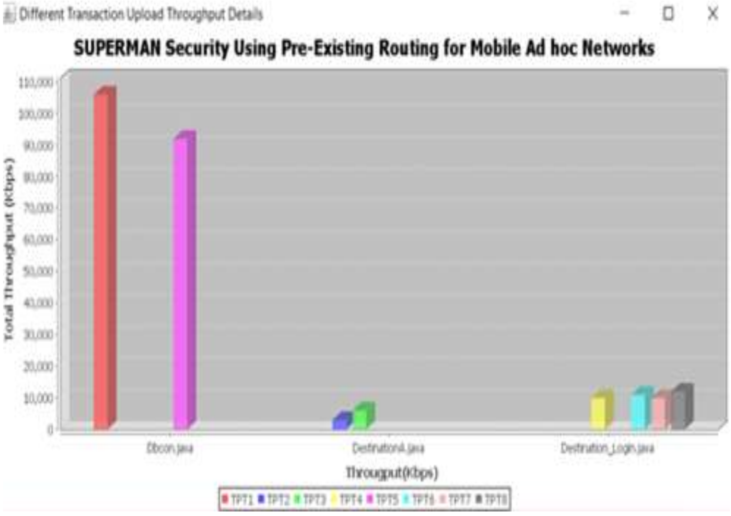

Fig.2.Different Transaction Upload Throughput Details

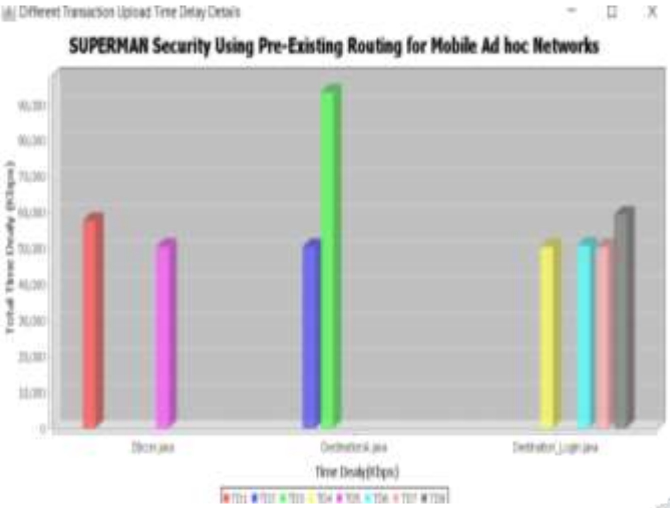

Fig.3.Different Transaction Upload Time delay Details

6.Conclusion

SUPERMAN is a novel security framework that protects the network and communication in MANETs. The primary focus is to secure access to a virtually closed network (VCN) that allows expedient, reliable communication with confidentiality, integrity and authenticity services. SUPERMAN addresses all eight security dimensions outlined in X.805. Thus, SUPERMAN can be said to implement a full suite of security services for autonomous MANETs. It fulfils more of the core services outlined in X.805 than IPsec, due to being network focused instead of end to- end oriented.

IPsec is intended to provide a secure environment between two end-points regardless of route, and has been suggested by some researchers to be a viable candidate for MANET security.

Simulation has been undertaken and the results are reported and analyzed to determine the relative cost of security for SUPERMAN, compared against IPsec, SAODV and SOLSR where relevant.

SUPERMAN provides a VCN, in which the foundation block of security is provided by authenticating nodes with the network. This enables further benefits, such as the security association referral and network merging. It also provides a relatively light-weight encapsulation packet and variable length tag.

Under both CBBA and CF-CBBA, the security overheads of SUPERMAN have been demonstrated to be lower than those of IPsec. Both DTA algorithms represent how a MANET can be made autonomous, by allowing problem solving without human intervention to occur on the network. Securing the communication required to facilitate this functionality is a critical consideration when providing a fully secured network. By providing lower cost security than existing alternatives, while providing security across all eight security dimensions, SUPERMAN proves it is a viable and competitive approach to securing the communication required by autonomous MANETs. SUPERMAN has been shown to provide lower-cost security than SAODV and SOLSR for their respective routing protocols. By establishing a secure, closed network; one can assume a certain level of trust within that network. This reduces the need for costly secure routing designed to mitigate the effects of an untrusted environment (and untrusted nodes) on the routing process. SUPERMAN provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs, it is not suitable for use in other types of network at this time. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes.

Future work includes the implementation of SUPERMAN on a simple mobile node platform to allow experimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing SUPERMAN services between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on SUPERMAN to better understand the role of the credential referral mechanism on overhead mitigation in SUPERMAN networks.

7.REFERENCES

[1] Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle IEEE Transactions on Mobile Computing,Volume:16,Issue:10,Issue Date:Oct.1.2017.

[2] P. S. Kiran, “Protocol architecture for mobile ad hoc networks,” 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.

[3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, “A cluster-based approach to consensus based distributed task allocation,” in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.

[5] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, “Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.

[6] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, “Performance analysis of mesh routing protocols for uav swarming applications,” in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.

[7] Shamsul Jamel Elias, Mohd Nazri Bin Mohd Warip, R Badlishah Ahmad, Aznor Hanah Abdul Halim A Comparative Study of IEEE 802.11 Standards for Non-Safety Applications on Vehicular Ad Hoc Networks: A Congestion Control Perspective WCECS2014, vol. 2, pp.719-723

[8] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, “An evaluation of protocols for uav science applications,” 2011.

[9] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, “Dos attacks in mobile ad hoc networks: A survey,” in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012, pp. 535–541.

[10] S. Maity and S. K. Ghosh, “Enforcement of access control policy for mobile ad hoc networks,” in Proceedings of the Fifth International Conference on Security of Information and Networks. ACM, 2012, pp. 47–52.

[11] D. Hurley-Smith, J. Wetherall, and A. Adekunle, “Virtual closed networks: A secure approach to autonomous mobile ad hoc networks,” in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015, pp. 391–398.

[12] S. Bhattacharya and T. Basar, “Game-theoretic analysis of an aerial jamming attack on a uav communication network,” in American Control Conference (ACC), 2010. IEEE, 2010, pp. 818–823.

[13] S. Zhao, R. Kent, and A. Aggarwal, “A key management and secure routing integrated framework for mobile ad-hoc networks,” Ad Hoc Networks, vol. 11, no. 3, pp. 1046–1061, 2013.

[14] K. N. Ali, M. Basheeruddin, S. K. Moinuddin, and R. Lakkars, “Manipsec-ipsec in mobile ad-hoc networks,” in Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 1. IEEE, 2010, pp. 635–639.

[15] H. Krawczyk and P. Eronen, “Hmac-based extract and-expand key derivation function (hkdf),” 2010.

[16] A. Adekunle and S. Woodhead, “An aead cryptographic framework and tiny aead construct for secure wsn communication,” in Wireless Advanced (WiAd), 2012. IEEE, 2012, pp. 1–5.