



بخشی از ترجمه مقاله

عنوان فارسی مقاله :

تحلیل الزامات, حملات و آسیب پذیری های امنیتی در لایه انتقال
شبکه های حسگر بی سیم

عنوان انگلیسی مقاله :

Analysis of Security Requirements, Attacks and Vulnerabilities
at Transport Layer in Wireless Sensor Networks



توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل
با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، [اینجا](#) کلیک نمایید.



بخشی از ترجمه مقاله

10. CONCLUSION

There are various attacks to hamper the smooth functioning of wireless sensor networks like denial of sleep, homing etc. In many situations, attacks may overlap also with each other. It is difficult to measure the attacks and their solution at physical layer as sensors have native radios of very low power and are operated in open area, unattended environment, hence are very poor to resist such attacks. Though there are algorithms and security mechanisms for network security and protection from above attacks but cannot be applied in WSN nodes due to node's constraints. There is need of tiny low computational algorithms for WSN. However there are many algorithms existing for WSN infrastructure and being applied also. But those are failure to be proved as correct and fruitful measures against above attacks. DoS situation at any layer in WSN requires to be addressed by strong mechanism. It is recommended to develop a prevention scheme against attacks which can be applied already to make WSNs. much stronger against DoS attacks. DoS may appear as individual and sometime altogether. It is always advisable to develop and deploy a proper suitable measure in WSN as prevention already.

۱۰. نتیجه گیری

حملات مختلفی برای مختل نمودن کارکرد یکنواخت شبکه های حسگر بی سیم مانند انکار خواب، تعقیب و ردیابی و غیره وجود دارد. در بسیاری از وضعیت ها، حملات می توانند با یکدیگر تداخل داشته باشند. اندازه گیری حملات و راه حل آنها در لایه فیزیکی مشکل است. زیرا حسگرها دارای رادیوهای بومی با توان بسیار پایین هستند و در ناحیه باز، محیط آزاد عمل می کنند و از اینرو مقاومت در برابر چنین حملاتی، ضعیف است. هرچند الگوریتم ها و مکانیزم های امنیتی برای امنیت و حفاظت از شبکه در برابر حملات بالا وجود دارند اما به دلیل محدودیت های گره، نمی توانند در گره های WSN به کار برده شوند. نیاز به الگوریتم های محاسباتی بسیار ریز برای WSN وجود دارد. هرچند، بسیاری از الگوریتم های موجود برای زیرساخت WSN وجود دارند و نیز اعمال می شوند. اما خرابی هایی در اقدامات فربخش و صحیح در برابر حملات بالا نیز اثبات شده است. وضعیت DoS در هر لایه در WSN باید توسط یک مکانیزم قوی رسیدگی شود. توسعه یک طرح جلوگیری در برابر حملاتی که می توانند از قبل برای قوی ساختن WSN ها در برابر حملات DoS به کار برده شوند، توصیه می شود. DoS می تواند به صورت فردی و برخی اوقات به صورت گروهی ظاهر شود. همیشه توسعه و به کارگیری یک اقدام مناسب در WSN به عنوان پیشگیری توصیه می شود.



توجه!

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، [اینجا](#) کلیک نمایید.

برای جستجوی جدیدترین مقالات ترجمه شده، [اینجا](#) کلیک نمایید.